CA Process Automation

Manuel d'installation

Version 04.2.00

La présente Documentation, qui inclut des systèmes d'aide et du matériel distribués électroniquement (ci-après nommés "Documentation"), vous est uniquement fournie à titre informatif et peut être à tout moment modifiée ou retirée par CA. La présente Documentation est la propriété exclusive de CA et ne peut être copiée, transférée, reproduite, divulguée, modifiée ou dupliquée, en tout ou partie, sans autorisation préalable et écrite de CA.

Si vous êtes titulaire de la licence du ou des produits logiciels décrits dans la Documentation, vous pourrez imprimer ou mettre à disposition un nombre raisonnable de copies de la Documentation relative à ces logiciels pour une utilisation interne par vous-même et par vos employés, à condition que les mentions et légendes de copyright de CA figurent sur chaque copie.

Le droit de réaliser ou de mettre à disposition des copies de la Documentation est limité à la période pendant laquelle la licence applicable du logiciel demeure pleinement effective. Dans l'hypothèse où le contrat de licence prendrait fin, pour quelque raison que ce soit, vous devrez renvoyer à CA les copies effectuées ou certifier par écrit que toutes les copies partielles ou complètes de la Documentation ont été retournées à CA ou qu'elles ont bien été détruites.

DANS LES LIMITES PERMISES PAR LA LOI APPLICABLE, CA FOURNIT LA PRÉSENTE DOCUMENTATION "TELLE QUELLE", SANS AUCUNE GARANTIE, EXPRESSE OU TACITE, NOTAMMENT CONCERNANT LA QUALITÉ MARCHANDE, L'ADÉQUATION À UN USAGE PARTICULIER, OU DE NON-INFRACTION. EN AUCUN CAS, CA NE POURRA ÊTRE TENU POUR RESPONSABLE EN CAS DE PERTE OU DE DOMMAGE, DIRECT OU INDIRECT, SUBI PAR L'UTILISATEUR FINAL OU PAR UN TIERS, ET RÉSULTANT DE L'UTILISATION DE CETTE DOCUMENTATION, NOTAMMENT TOUTE PERTE DE PROFITS OU D'INVESTISSEMENTS, INTERRUPTION D'ACTIVITÉ, PERTE DE DONNÉES OU DE CLIENTS, ET CE MÊME DANS L'HYPOTHÈSE OÙ CA AURAIT ÉTÉ EXPRESSÉMENT INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES OU PERTES.

L'utilisation de tout produit logiciel mentionné dans la Documentation est régie par le contrat de licence applicable, ce dernier n'étant en aucun cas modifié par les termes de la présente.

CA est le fabricant de la présente Documentation.

Le présent Système étant édité par une société américaine, vous êtes tenu de vous conformer aux lois en vigueur du Gouvernement des Etats-Unis et de la République française sur le contrôle des exportations des biens à double usage et aux autres réglementations applicables et ne pouvez pas exporter ou réexporter la documentation en violation de ces lois ou de toute autre réglementation éventuellement applicable au sein de l'Union Européenne.

Copyright © 2013 CA. Tous droits réservés. Tous les noms et marques déposées, dénominations commerciales, ainsi que tous les logos référencés dans le présent document demeurent la propriété de leurs détenteurs respectifs.

Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

Modifications de la documentation

Les mises à jour suivantes de la documentation ont été faites depuis la dernière publication de cette documentation :

- Que souhaitez-vous réaliser (page 13) ? : cette rubrique existante porte un nouveau nom et contient désormais uniquement des liens vers diverses tâches d'installation.
- Introduction aux composants d'un système CA Process Automation (page 15) : ce nouveau chapitre décrit chaque composant, en premier lieu ceux qui sont requis pour la configuration d'un système simple.
  - Système CA Process Automation simple (page 15)
  - Système CA Process Automation standard (page 17)
  - Système CA Process Automation mis en cluster (page 19)
  - Associations standard de bases de données (page 20)
- Les rubriques suivantes ont été mises à jour pour indiquer que seule la version 1.7 du JDK est prise en charge dans CA Process Automation 4.2. Cette condition préalable s'applique aux orchestrateurs uniquement. CA Process Automation prend en charge la version Java 6 d'un environnement d'exécution Java (jusqu'à JRE 1.6.0_45) pour des agents.
  - Prise en charge des plates-formes et conditions requises pour les composants CA Process Automation (page 30)
  - Configuration requise pour le kit de développement Java (page 77)
  - Remarques concernant la base de données lors de la mise à niveau de CA IT PAM 2.x vers CA Process Automation 4.2
  - Mise à niveau vers le kit de développement Java 1.7
  - Mise à niveau vers CA Process Automation 4.2
- Directives pour la spécification du nom de serveur de base de données pour SQL Server : (page 75) cette nouvelle rubrique traite de l'hébergement d'une base de données CA Process Automation sur une instance nommée SQL Server.
- Droits de propriétaire de base de données (page 76) : cette rubrique existante a été corrigée et inclut désormais les droits d'action sur les vues.
- Installation de l'orchestrateur de domaine (page 96): cette rubrique existante a été mise à jour et contient désormais les nouvelles pages ajoutées à l'assistant d'installation de cette version.
- Installation interactive d'un agent (page 176) : cette rubrique existante a été mise à jour et contient désormais des informations sur une nouvelle case à cocher permettant de spécifier si l'agent doit utiliser la communication simplifiée sur des ports Internet standard (par défaut) ou la communication désapprouvée sur le port 7003.

- Prise en charge de la post-installation lors des mises à niveau de CA EEM (page 167) : cette nouvelle rubrique décrit la procédure de mise à niveau d'une version 4.2 existante de CA Process Automation lors de la mise à niveau de la version de compilation de CA EEM ou de la génération de nouveaux certificats dont les longueurs de clé sont plus longues.
- Exemple de scénario : configuration de l'installation existante pour régénérer les certificats CA Process Automation : (page 162) cette nouvelle rubrique contient la procédure d'installation à suivre si l'administrateur de CA EEM régénère les certificats avec des clés de 2 048 ou 4 096 bits après l'installation de CA Process Automation avec CA EEM r12.51.
- Conditions requises pour l'équilibreur de charge F5 (page 53) : cette section existante a été modifiée et contient désormais les changements apportés pour la prise en charge de la communication simplifiée et la suppression de références au noeud principal. D'autres changements ont été apportés pour améliorer la facilité d'utilisation.
- Equilibreur de charge NGINX : (page 35) cette nouvelle section décrit la procédure de configuration de l'équilibreur de charge NGINX, qui prend en charge la communication simplifiée. Cet équilibreur de charge constitue une alternative à Apache appropriée, qui prend en charge uniquement les communications désapprouvées.
- A propos des communications d'agent (page 159) : cette nouvelle rubrique décrit la nouvelle méthode de communication simplifiée.

- Procédure de mise à niveau de CA Process Automation (page 142): ce nouveau scénario a été ajouté au chapitre Mise à niveau vers la version actuelle.
  - Exécution de sauvegardes et préparation en cas d'interruption (page 143) : cette nouvelle rubrique est basée sur l'expérience réelle de mise à niveau par un client.
  - Conditions préalables requises pour la mise à niveau (page 145)
  - Procédure de mise à niveau de l'orchestrateur de domaine (page 146)
  - Procédure de mise à niveau d'un orchestrateur de domaine non mis en cluster (page 150)
  - Procédure de mise à niveau d'un noeud de cluster (page 153)
  - Réalisation de tâches postérieures à la mise à niveau (page 156) : cette nouvelle rubrique inclut des conseils en lien avec l'expérience réelle de mise à niveau par un client.
  - Test de vos processus avec les orchestrateurs mis à niveau (page 157)
  - Basculement de l'équilibreur de charge Apache vers l'équilibreur de charge NGINX (page 158)
  - Mise à jour des pools F5, de la définition d'iRule et de la configuration (page 158)
  - Configuration des agents pour utiliser la communication simplifiée (page 159)
  - Test de vos processus avec la communication simplifiée (page 160)
- Exemples de mise à niveau : cette nouvelle annexe inclut les exemples suivants :
  - Exemple de mise à niveau d'un orchestrateur non mis en cluster de la version 4.1sp01 vers la version 4.2 (page 292) : cette nouvelle rubrique contient des captures d'écran spécifiques à ce scénario de mise à niveau.
  - Exemple de mise à niveau d'un noeud de l'orchestrateur de domaine de la version 3.1sp01 vers la version 4.2 (page 281) : cette nouvelle rubrique contient des captures d'écran spécifiques à ce scénario de mise à niveau.
  - Exemple de mise à niveau d'un autre noeud de l'orchestrateur de domaine de la version 3.1sp01 vers la version 4.2 (page 289) : cette nouvelle rubrique contient des captures d'écran spécifiques à ce scénario de mise à niveau.
- Ports utilisés par CA Process Automation (page 227) : cette nouvelle annexe répertorie les ports utilisés par chaque composant d'un système CA Process Automation standard.

Table des matières

Chapitre 1: Que souhaitez-vous réaliser ? 13

Chapitre 2: Introduction aux composants d'un système CA Process Automation 15

Système CA Process Automation simple 15
Système CA Process Automation standard 17
Système CA Process Automation mis en cluster 19
Options de configuration avancée 20
Exemple : Activation de la portabilité de contenu par les points de contact 24
Téléchargement de la bibliothèque CA Process Automation sans accès à Internet 26

Chapitre 3: Prise en charge des plates-formes et configuration matérielle requise 29

Prise en charge des plates-formes et conditions requises pour les composants CA Process Automation 30
Configuration matérielle requise 32

Chapitre 4: Configuration d'un équilibreur de charge pour la mise en cluster d'un orchestrateur 35

Equilibreur de charge NGINX 35
- Configuration requise 36
- Communication simple 38
- Communication sécurisée 42
- Configuration d'REST 47
- Génération de fichiers de certificat SSL 50

Conditions requises pour l'équilibreur de charge F5 53
- Création d'un noeud F5 pour chaque noeud de cluster 54
- Création de deux pools F5 pour chaque cluster CA Process Automation 55
- Création d'une iRule F5 pour CA Process Automation 56
- Création d'un serveur virtuel F5 pour CA Process Automation 59
- Configuration de F5 pour utiliser la communication simplifiée HTTPS 61
- Préparation de l'équilibreur de charge F5 pour la vérification de la communication (exemple) 63

Chapitre 5: Installation de l'orchestrateur de domaine 65

Conditions préalables à l'installation de l'orchestrateur de domaine 65
- Détermination de l'emplacement des composants pris en charge 67

Conditions requises pour le serveur de base de données 69
Configuration requise pour le kit de développement Java 77
Conditions préalables pour CA EEM 79
Conditions préalables la planification des ports 93
Installation interactive de l'orchestrateur de domaine 93
Installation du logiciel Third-Party 94
Installation de l'orchestrateur de domaine 96
Installation autonome de l'orchestrateur de domaine 118
Création d'un fichier de réponse 118
Exécution ou modification du fichier de script d'installation silencieuse 121
Remarques concernant la mise à niveau (installation silencieuse) 124
Tâches de post-installation liées à l'orchestrateur de domaine 125
Accès à CA Process Automation et connexion en tant qu'administrateur par défaut 126
Mise à disposition de la bibliothèque pour les utilisateurs sans accès à Internet 128
Activation de la communication bidirectionnelle au niveau du pare-feu 129
Installation des pilotes pour les opérateurs de base de données 130
Activation de l'authentification directe NTLM après l'installation 131
Interaction avec la configuration du bureau 132
Configuration de CA EEM pour permettre aux utilisateurs référencés de se connecter avec une adresse électronique 132
Conditions préalables à la synchronisation horaire 134
Procédure d'installation des patchs et des connecteurs avec CA Process Automation 4.2 134
Modification de la configuration du serveur de base de données Oracle pour utiliser RAC Oracle 136
Arrêt de l'orchestrateur 138
Démarrage de l'orchestrateur 139
Désinstallation de l'orchestrateur de domaine 140

Chapitre 6: Mise à niveau vers la version actuelle 141

Procédure de mise à niveau de CA Process Automation 142
Exécution de sauvegardes et préparation en cas d'interruption 143
Conditions préalables requises pour la mise à niveau 145
Procédure de mise à niveau de l'orchestrateur de domaine 146
Procédure de mise à niveau d'un orchestrateur de domaine non mis en cluster 150
Procédure de mise à niveau d'un noeud de cluster 153
Réalisation des tâches postérieures à la mise à niveau 156
Test de vos processus avec les orchestrateurs mis à niveau 157
Basculement de l'équilibreur de charge Apache vers l'équilibreur de charge NGINX 158
Mise à jour des pools F5, de la définition d'iRule et de la configuration 158
Configuration des agents pour utiliser la méthode de communication simplifiée 159
A propos des communications d'agent 159
Test de vos processus avec la communication simplifiée 160

Chapitre 7: Réinstallation ou configuration de la version actuelle 161

Exemple de scénario : configuration de l'installation existante pour régénérer les certificats CA Process Automation 162
Prise en charge de la post-installation lors des mises à niveau de CA EEM 167
Activation de la communication sécurisée pour la version existante de CA Process Automation 171

Chapitre 8: Installation des agents 173

Conditions préalables à l'installation des agents 173
Identification des hôtes qui ont besoin des agents 173
Vérification des conditions Java requises pour les agents 174
Détermination des ports disponibles pour l'agent 174
Accès et connexion à CA Process Automation 175
Installation interactive d'un agent 176
Exécution d'une installation autonome d'agents 179
Tâches de post-installation des agents 183
Résolution du conflit de ports pour un agent 184
Configuration des agents pour une exécution en tant qu'utilisateur à faibles privilèges standard 185
Démarrage et arrêt d'un agent 186

Chapitre 9: Ajout d'un noeud à l'orchestrateur de domaine 189

Conditions préalables à l'installation d'un noeud de cluster pour l'orchestrateur de domaine 190
Installez un noeud de cluster pour l'orchestrateur de domaine 193
Synchronisation horaire d'un noeud de cluster 195

Chapitre 10: Installation d'un orchestrateur supplémentaire 197

Conditions préalables à l'installation d'un orchestrateur 197
Installation d'un orchestrateur 200
Tâches de post-installation d'un orchestrateur 206

Chapitre 11: Ajout d'un noeud à un orchestrateur supplémentaire 207

Conditions préalables à l'installation d'un noeud de cluster pour un orchestrateur 208
Installation d'un noeud de cluster pour un orchestrateur 211
Synchronisation horaire d'un noeud de cluster 213

Chapitre 12: Réglage de CA Process Automation 215

Amélioration des performances de CA Process Automation 216

Annexe A: Utilisation de CA SiteMinder avec CA Process Automation 219

Conditions requises pour CA SiteMinder 220
Configuration des objets de serveur de politiques CA SiteMinder 220
Intégrez CA Process Automation avec IIS pour l'authentification unique 222
Configuration de l'hôte IIS pour la redirection des demandes vers Tomcat 223
Intégrer CA Process Automation avec Apache pour l'authentification unique 225
Activer la déconnexion dans CA Process Automation pour l'authentification unique 226

Annexe B: Ports utilisés par CA Process Automation 227

Communications dans une architecture standard 228
Ports utilisés par CA EEM 229
Ports utilisés par l'équilibreur de charge 231
Ports utilisés par un orchestrateur 234
Ports utilisés par un agent 242
Ports utilisés par les serveurs de base de données 244
Ports utilisés par les clients Web 245

Annexe C: Conservation du nom DNS ou de l'adresse IP de l'orchestrateur 247

Maintenance des adresses IP 247
Résolution des caractères non valides dans le nom DNS de CA Process Automation 248
- Activation du DNS pour résoudre un nom d'hôte non valide 248
- Conservation du nom d'hôte DNS 249
- Syntaxe des noms d'hôte DNS 250

Annexe D: Dépannage 251

Echec d'installation de CA Process Automation 251
Problème possible lors de l'exécution de CA Process Automation sur un serveur VMware avec une interface réseau E1000 252
Bug Oracle n° 9347941 254
Restrictions dans Internet Explorer 255
Installation de CA Process Automation dans des environnements réseau à double pile (IPv4 et IPv6) 256
Performances lentes avec MySQL 256
Impossible de créer la base de données d'exécution 258
Impossible d'exécuter des opérateurs Exécuter le script ou Exécuter le programme sur RHEL6 259

Annexe E: Equilibreur de charge Apache 261

Conditions requises pour l'équilibreur de charge Apache 261
Configuration de l'équilibreur de charge Apache sur Windows 261
- Configuration de base (Windows) 262

Configuration sécurisée (Windows) 266
Configuration de l'équilibreur de charge Apache sur un système d'exploitation autre que Windows 271
Configuration de base (système d'exploitation autre que Windows) 272
Configuration sécurisée (système d'exploitation autre que Windows) 276

Annexe F: Exemples de mise à niveau 281

Exemple : mise à niveau d'un noeud de l'orchestrateur de domaine de la version 3.1 SP01 vers 4.2 sous Windows 281
Exemple : mise à niveau d'un autre noeud de l'orchestrateur de domaine de la version 3.1 SP01 vers 4.2 sous Windows 289
Exemple : mise à niveau d'un orchestrateur non mis en cluster de 4.1 SP01 vers 4.2 sous Windows 292
Mise à niveau d'une version antérieure vers 3.1 SP01 298

Chapitre 1: Que souhaitez-vous réaliser ?

- **Effectuer la première installation de CA Process Automation**
  - Introduction aux composants d'un système CA Process Automation (page 15)
  - Prise en charge des plates-formes et configuration matérielle requise (page 29)
  - Installation de l'orchestrateur de domaine (page 65)
- **Mise à niveau de CA Process Automation à partir d'une version antérieure** (page 141)
- Mise à jour de la version actuelle de CA Process Automation aux fins suivantes :
  - Utilisation de plusieurs domaines Microsoft Active Directory (page 167) (après la mise à niveau de CA EEM vers la version 12.5)
  - Utilisation de nouveaux certificats de CA EEM 12.5 (page 162) (avec une version existante de CA EEM 12.5)
  - Activation des communications sécurisées (HTTPS) (page 171)
  - Utilisation d'une nouvelle adresse IP d'hôte (page 247)
- Installation d'un agent (page 173)
- Création de votre système
  - Configuration d'un équilibreur de charge pour la mise en cluster de l'orchestrateur (page 35)
  - Ajout d'un noeud à l'orchestrateur de domaine (page 189)
  - Installation d'un orchestrateur supplémentaire (page 197)
  - Ajout d'un noeud à un orchestrateur supplémentaire (page 207)
- Dépannage (page 251)
- Utilisation de CA SiteMinder avec CA Process Automation (page 219)

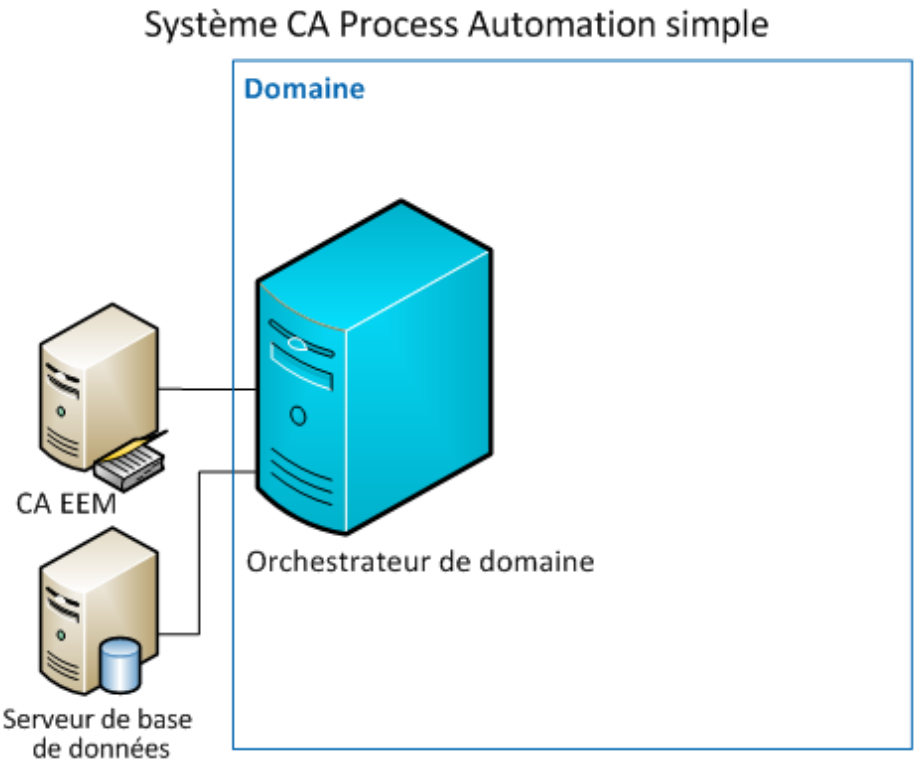
Chapitre 2: Introduction aux composants d'un système CA Process Automation

Ce chapitre traite des sujets suivants :

Système CA Process Automation simple (page 15)
Système CA Process Automation standard (page 17)
Système CA Process Automation mis en cluster (page 19)
Options de configuration avancée (page 20)
Exemple : Activation de la portabilité de contenu par les points de contact (page 24)
Téléchargement de la bibliothèque CA Process Automation sans accès à Internet (page 26)

Système CA Process Automation simple

Un système CA Process Automation simple inclut trois composants : l'orchestrateur de domaine, un serveur de base de données et le produit CA Embedded Entitlements Manager (CA EEM).



L'orchestrateur de domaine

Les orchestrateurs sont des serveurs CA Process Automation. Les utilisateurs se connectent à un orchestrateur pour concevoir et tester des processus, exécuter des processus et configurer le système CA Process Automation de diverses manières. Tous les systèmes CA Process Automation contiennent un orchestrateur de domaine et peuvent également contenir un ou plusieurs autres types d'orchestrateur. Un déploiement simple contient un seul orchestrateur de domaine.

Un serveur de base de données

Lors de l'installation de l'orchestrateur de domaine, identifiez le serveur de base de données dans lequel les trois bases de données CA Process Automation seront créées.

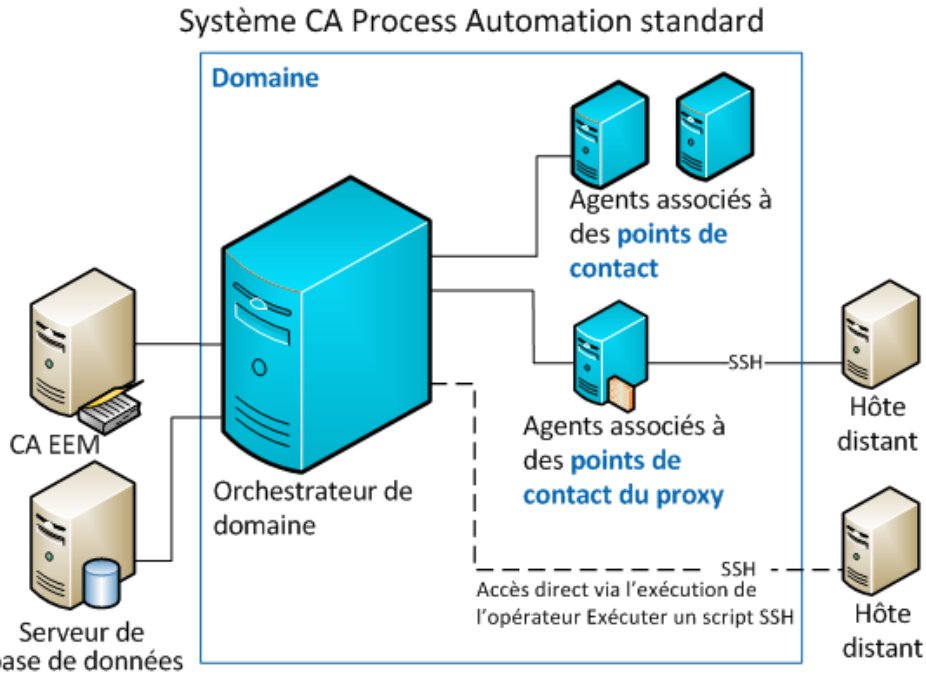
- La base de données de bibliothèque stocke le contenu d'automatisation que vous créez, par exemple des processus, des ensembles de données ou des formulaires.
- La base de données d'exécution stocke les informations sur les états des instances de processus exécutées ou en cours d'exécution.
- La base de données de reporting stocke des informations sur les instances de processus exécutées dans un format adapté à l'exécution de rapports.

CA Embedded Entitlements Manager (CA EEM)

- Lors de l'installation de l'orchestrateur de domaine, enregistrez l'application CA Process Automation dans CA EEM. Vous pouvez utiliser une seule instance de CA EEM unique avec plusieurs produits CA Technologies pour concentrer en un seul lieu la gestion des identités des utilisateurs et leurs autorisations d'accès à l'application.
- CA EEM permet d'authentifier les utilisateurs CA Process Automation. CA EEM tente d'établir des correspondances entre les informations d'identification saisies par les utilisateurs lorsqu'ils se connectent et les informations d'identification d'utilisateurs CA Process Automation connus. Toutes les informations d'identification valides sont directement définies dans CA EEM, ou, en règle générale, référencées par CA EEM à partir d'un ou plusieurs référentiels LDAP tels que Microsoft Active Directory.
- CA EEM gère également les niveaux d'autorisation des utilisateurs CA Process Automation. Dans CA EEM, vous affectez des autorisations à chaque compte d'utilisateur après l'installation de CA Process Automation, de sorte à fournir aux utilisateurs les autorisations pertinentes dans l'application CA Process Automation.

Système CA Process Automation standard

De nombreux déploiements requièrent la capacité de distribuer une certaine charge de travail à exécuter sur des hôtes autres que l'orchestrateur de domaine. Vous pouvez exécuter certains types de charge de travail sur un hôte distant sans agent. Toutefois, d'autres fonctionnalités sont disponibles lorsqu'un agent CA Process Automation est installé sur l'hôte cible.


Système CA Process Automation standard
Domaine
Agents associés à des points de contact
CA EEM
Orchestrateur de domaine
Agents associés à des points de contact du proxy
SSH
Hôte distant
Serveur de base de données
SSH
Accès direct via l'exécution de l'opérateur Exécuter un script SSH
Hôte distant

Agents

Chaque instance de processus consiste en un ou plusieurs opérateurs. Chaque opérateur est ciblé pour être exécuté sur un hôte spécifique, de manière directe ou indirecte à l'aide du concept de points de contact. Chaque point de contact est mappé vers un hôte spécifique dans la configuration du système.

Le même nom de point de contact peut être mappé vers différents hôtes dans différents domaines ou environnements CA Process Automation. Ainsi, les points de contact permettent au même contenu de processus d'être déployé sans être modifié dans différents domaines ou environnements CA Process Automation.

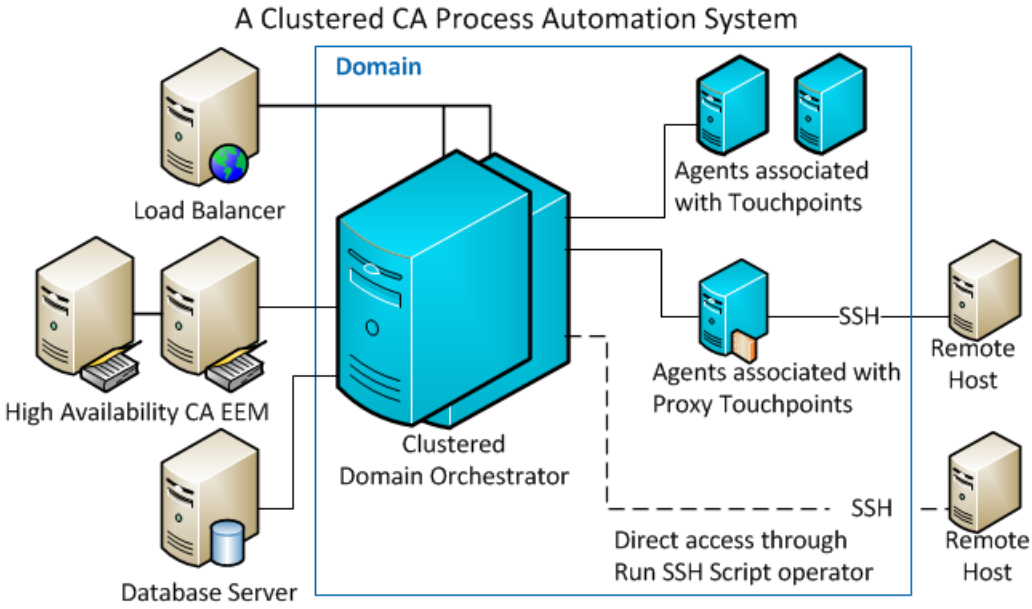
Les points de contact peuvent être mappés vers un orchestrateur CA Process Automation ou un agent CA Process Automation. Les points de contact de proxy sont mappés vers un hôte distant sans logiciel CA Process Automation. Les orchestrateurs peuvent distribuer la charge de travail vers un hôte distant en s'y connectant directement via SSH, ou via un agent, qui lui-même se connecte à l'hôte distant via SSH.

A la manière d'un point de contact, un point de contact du proxy est une entité logique. Il s'agit d'un nom que vous pouvez utiliser dans le concepteur de processus pour spécifier une cible d'exécution d'un opérateur. Lors de la définition d'un point de contact et de son mappage vers un agent spécifique dans la configuration de l'environnement, un point de contact du proxy est mappé vers un hôte distant spécifique sans agent. Chaque hôte distant sans agent (mappé vers un point de contact du proxy) est géré par un agent installé sur un hôte différent. Lorsqu'un orchestrateur distribue le travail qui cible un point de contact du proxy, il envoie le travail à l'agent qui gère l'hôte distant et qui établit lui-même une session SSH vers l'hôte distant pour exécuter le travail.

Par conséquent, la tâche principale d'un agent CA Process Automation est d'exécuter la charge de travail sur l'hôte sur lequel il est installé. De plus, les agents peuvent servir de passerelle à travers laquelle la charge de travail est distribuée vers des hôtes distants sur lesquels vous ne pouvez pas installer d'agent.

Système CA Process Automation mis en cluster

De nombreuses installations déploient un orchestrateur de domaine mis en cluster pour la haute disponibilité et la modularité du déploiement.



Orchestrateurs mis en cluster

Un orchestrateur mis en cluster consiste en deux ou plusieurs noeuds. Lors d'opérations habituelles, la charge de travail est répartie parmi les noeuds de l'orchestrateur. Vous pouvez ajouter des noeuds supplémentaires pour accroître la capacité de l'orchestrateur si nécessaire. En cas d'échec d'un noeud de l'orchestrateur, les autres noeuds reprennent les responsabilités du noeud en échec jusqu'à sa récupération, en fournissant la haute disponibilité.

Chaque noeud de l'orchestrateur est installé sur un hôte distinct. Installez et procédez à la mise à niveau de chaque noeud séparément.

Remarque : Si vous avez préalablement installé un orchestrateur dans une configuration autonome, vous devrez réexécuter l'assistant d'installation pour le reconfigurer en tant que noeud d'orchestrateur mis en cluster.

Equilibreur de charge

CA Process Automation prend en charge les équilibreurs de charge matérielle et logicielle, par exemple :

- F5
- NGINX
- Apache (avec des restrictions fonctionnelles)

Remarque : L'équilibreur de charge Apache est pris en charge pour la communication entre des agents mis à niveau et un orchestrateur mis en cluster. Toutefois, l'équilibreur de charge Apache ne prend pas en charge le protocole requis par le mécanisme de communication simplifiée. Vous pouvez continuer d'utiliser le modèle de communication désapprouvée avec Apache, mais si vous prévoyez d'exécuter un déploiement à l'aide d'un équilibreur de charge logicielle, il est vivement recommandé d'utiliser NGINX.

CA EEM pour la haute disponibilité

Vous pouvez configurer CA EEM avec un noeud de basculement pour réaliser des déploiements requérant une configuration de haute disponibilité complète.

Options de configuration avancée

Orchestrateurs autres que de domaine

Vous pouvez partitionner la charge de travail d'automatisation en déployant d'autres orchestrateurs. A l'instar des orchestrateurs de domaine, les orchestrateurs d'autres types peuvent être mis en cluster.

Par exemple, vous devez cibler l'exécution d'une certaine charge de travail dans un centre de données ou une région spécifique et la configuration du système CA Process Automation doit être différente dans chaque emplacement. Une solution consisterait à déployer un orchestrateur dans chaque centre de données et d'utiliser la configuration de niveau orchestrateur pour remplacer la configuration de niveau domaine de manière appropriée.

Environnements

Un déploiement standard comprend un domaine et un seul environnement, à savoir l'environnement par défaut.

Vous pouvez partitionner un domaine CA Process Automation en plusieurs environnements. Puis, vous pouvez adapter divers aspects de la configuration de domaine à chaque environnement. Par exemple, avec plusieurs environnements vous pouvez configurer des éléments d'une certaine manière dans un contexte de développement de contenu et d'une autre dans un contexte de test ou de production.

Chaque environnement peut disposer de sa propre Bibliothèque de sorte que vous pussiez utiliser des versions de contenu potentiellement différentes dans les différents environnements.

Les environnements peuvent également partitionner la charge de travail. Un orchestrateur spécifique est associé à un environnement. L'environnement par défaut comprend l'orchestrateur de domaine et peut inclure un ou plusieurs autres types d'orchestrateurs. Tous les autres environnements peuvent comprendre un ou plusieurs autres types d'orchestrateurs. Chaque orchestrateur de domaine et chaque autre type d'orchestrateur peut être mis en cluster (plusieurs noeuds) ou non (un seul noeud).

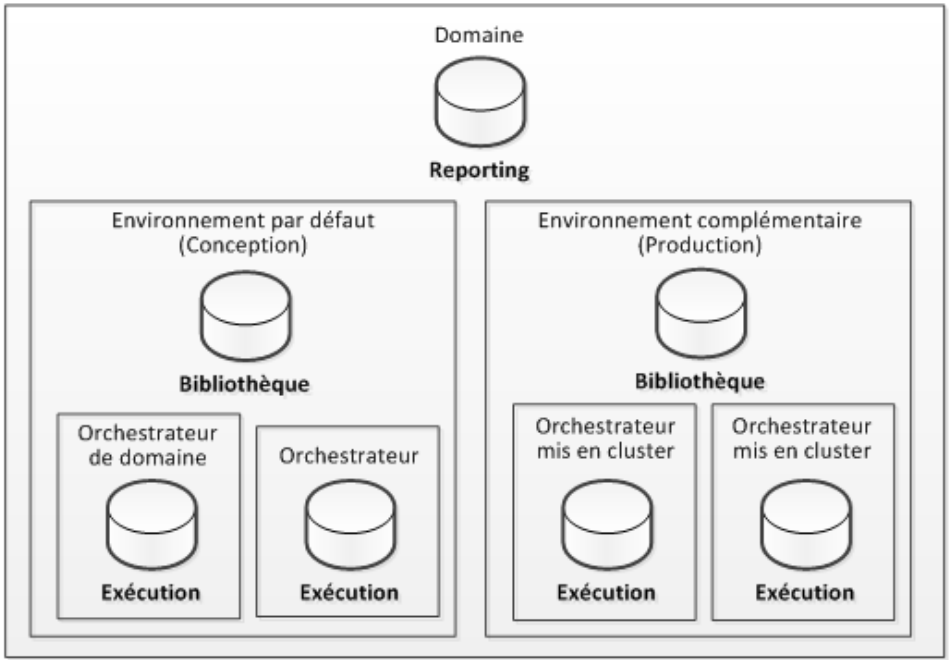
Les environnements peuvent également permettre de partitionner la charge de travail dans un contexte de production. Par exemple, un fournisseur de services peut déployer un environnement par client. Cette installation permet d'exécuter le même contenu d'automatisation standard dans plusieurs environnements dont la charge de travail est physiquement partitionnée. Ces environnements qui exécutent le même contenu sont configurés de manière différente et peuvent être exécutés dans différents emplacements géographiques.

Conséquences de l'ajout d'environnements et d'autres types d'orchestrateurs sur la base de données

L'affectation du partage des bases de données entre des orchestrateurs présente une certaine flexibilité. Voici des exemples d'association standard :

- Une seule base de données de reporting est partagée par tous les orchestrateurs présents dans le domaine. Bien que vous ne puissiez partager aucune base de données dans plusieurs domaines, vous pouvez utiliser plusieurs bases de données de reporting.
- Une base de données de bibliothèque pour tous les environnements, dans lesquels chaque base de données de bibliothèque est partagée par tous les orchestrateurs dans le même environnement
- Une base de données d'exécution par orchestrateur est une condition obligatoire. Chaque orchestrateur autonome (non mis en cluster) possède sa propre base de données d'exécution. De même, chaque orchestrateur mis en cluster utilise une seule base de données d'exécution.

Associations standard de bases de données



Dans un déploiement simple dont l'environnement par défaut comprend un orchestrateur de domaine non mis en cluster, les trois bases de données CA Process Automation sont installées sur un serveur de base de données.

L'ajout d'autres environnements et l'installation d'autres types d'orchestrateurs accroît de manière significative la complexité de la configuration de la base de données requise.

Informations complémentaires :

A propos des bases de données CA Process Automation (page 70)

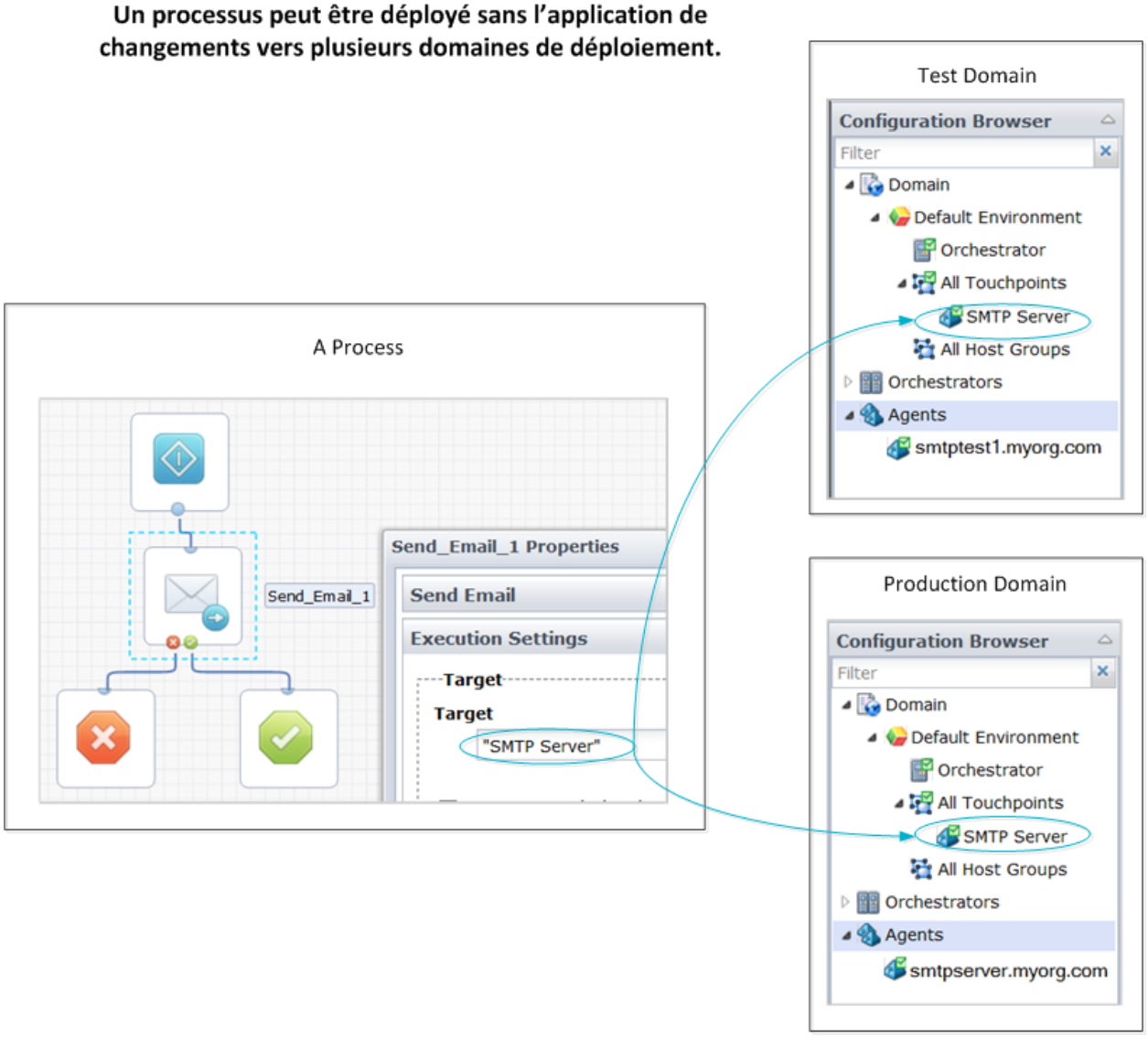
Exemple : Activation de la portabilité de contenu par les points de contact

Prenons par exemple un déploiement comprenant un domaine de test et un domaine de production, chacun d'eux disposant de son propre serveur SMTP.

- smtptest1.myorg.com dans le domaine de test
- smptserver.myorg.com dans le domaine de production

L'administrateur installe un agent sur chaque serveur SMTP et configure chacun des agents avec un point de contact nommé Serveur SMTP. Un concepteur de contenu crée un processus avec un opérateur Send_Email, dans lequel la cible d'exécution est définie sur le nom de point de contact **Serveur SMTP**. Vous pouvez déployer ce processus sans appliquer de changements au domaine de test et au domaine de production.

Remarque : Les Manuels et l'Aide en ligne de CA Process Automation décrivent la procédure permettant de réaliser la portabilité de contenu parmi les environnements d'un seul domaine.



Téléchargement de la bibliothèque CA Process Automation sans accès à Internet

Cette section décrit la procédure de téléchargement de la bibliothèque CA Process Automation sans accès à Internet.

Remarque : Pour accéder à la bibliothèque CA Process Automation, vous devez télécharger le fichier *bookshelf.zip* sur tous les noeuds CA Process Automation.

Procédez comme suit :

1. Utilisez les informations d'identification de l'administrateur pour vous connecter à un noeud CA Process Automation avec un accès à Internet.

   L'interface utilisateur de CA Process Automation s'ouvre.

2. Dans l'interface utilisateur CA Process Automation, cliquez sur le lien Bibliothèque de la liste déroulante Aide.

   La bibliothèque CA Process Automation s'ouvre.

3. Dans la page de la bibliothèque CA Process Automation, cliquez sur le lien *Télécharger la bibliothèque*.

   Une boîte de dialogue s'ouvre et vous invite à enregistrer le fichier .zip.

4. Créez un dossier *Bibliothèque* à l'emplacement suivant :

   <*server_loc*>\c2o\.c2orepository\

5. Créez un <*nom de dossier de paramètres régionaux*> basé sur la langue de la bibliothèque sélectionnée à l'emplacement suivant :

   <*server_loc*>\c2o\.c2orepository\bookshelf\

   Remarque : En fonction de la langue de bibliothèque sélectionnée, utilisez le <*nom de dossier de paramètres régionaux*> approprié comme suit :

   - Anglais : le <*nom de dossier de paramètres régionaux*> est *en_US.*
   - Allemand - *de_DE*
   - Espagnol - es_ES
   - Français - *fr_FR*
   - Italien - *it_IT*
   - Japonais - *ja_JP*
   - Portugais : *pt_BR*
   - Turc - *tr_TR*
   - Chinois - *zh_CN*

6. Décompressez le fichier .zip et placez les fichiers de la bibliothèque CA Process Automation dans le dossier local suivant :

<server_loc>\c2o\.c2orepository\bookshelf*<nom de dossier de paramètres régionaux>*\ bookshelf files.

Vous pouvez maintenant accéder aux fichiers de la bibliothèque CA Process Automation à partir du dossier local.

Chapitre 3: Prise en charge des plates-formes et configuration matérielle requise

Ce chapitre traite des sujets suivants :

Prise en charge des plates-formes et conditions requises pour les composants CA Process Automation (page 30)
Configuration matérielle requise (page 32)

Prise en charge des plates-formes et conditions requises pour les composants CA Process Automation

Le tableau ci-après résume les plates-formes prises en charge par les composants CA Process Automation.

Remarque : La prise en charge des systèmes d'exploitation et des logiciels répertoriés peut varier. Pour obtenir les dernières informations sur la prise en charge des versions, consultez la rubrique Compatibilities (compatibilités) sur le site support.ca.com.

Composant CA Process Automation	Systèmes d'exploitation pris en charge	Logiciels requis	Autres conditions requises
orchestrateur	Serveur Microsoft Windows 2003 R2 x64 SPx, 2008 x64 SPx, 2012 x64 Solaris SPARC 10 Solaris 11 Red Hat Enterprise Linux 5 x64, 6 x64 SPx CentOS Linux 6 x64	Kit de développement Java 1.7 **Remarque :** Le kit de développement Java 1.7 est également requis par la version 3.4 du connecteur Catalyst intégré. Catalyst prend en charge l'API REST et tous les connecteurs UCF.	Consultez la rubrique Conditions préalables à l'installation de l'orchestrateur de domaine (page 65).

Composant CA Process Automation	Systèmes d'exploitation pris en charge	Logiciels requis	Autres conditions requises
Agent	Serveur Microsoft Windows 2003 R2 x64 SPx, 2003 R2 x32 SPx, 2008 x64 SPx, 2012 x64 SuSE Linux Enterprise Server 10 x64,11 x32 SPx, 11 x64 SPx Solaris SPARC 9, 10 Solaris 10 x86 x32 bits, 11 Red Hat Enterprise Linux 5 x64, 6 x32 SPx, 6 x64 SPx CentOS Linux 6 x64 AIX 6.1, 7.1 HP-UX 11i V3 (Itanium)	L'une des versions suivantes de l'environnement d'exécution Java (JRE) prises en charge par le système d'exploitation : ■ Pour Windows, Solaris SPARC et Linux : Oracle JRE 1.6 et 1.7 ■ Pour AIX, l'environnement d'exécution Java 1.6 d'IBM ■ Pour HP-UX, la configuration minimale est 1.6_04. HP Java 1.6 (JRE). **Important :** N'utilisez pas l'environnement d'exécution Java 6, mises à jour 27 (1.6.0_27) à 29 (1.6.0_29). Un problème avec ces versions affecte les applications, y compris CA Process Automation qui utilise JDBC pour se connecter à Microsoft SQL Server. La base de données de bogue du SDN répertorie ce problème sous le numéro de bogue 7105007. La mise à jour 45 de Java 1.6 correspond à la dernière version Java 6 prise en charge par les agents CA Process Automation.	Pour les points de contact de proxy et les groupes d'hôtes, chaque hôte distant doit exécuter un serveur SSHv2. Un hôte distant UNIX doit avoir un shell ksh.
Serveur de base de données	Pour des informations sur les systèmes d'exploitation pris en charge, consultez la documentation du fournisseur.	La base de données relationnelle doit être l'une des bases suivantes : ■ MySQL r5.5 ■ Microsoft SQL Server 2005, 2008, 2008 R2, 2012 ■ Oracle 11g R2	Pour obtenir des informations détaillées, consultez la section Conditions requises pour le serveur de base de données (page 69). Pour Oracle, les versions 11.1.0.7, 11.2.0.2 ou les versions ultérieures sont recommandées.

Composant CA Process Automation	Systèmes d'exploitation pris en charge	Logiciels requis	Autres conditions requises
Serveur d'annuaire	Consultez la documentation CA EEM (CA Embedded Entitlements Manager).	CA Embedded Entitlements Manager (CA EEM) 8.4 SP4 ou CA EEM r12 à r12.51	
Interface utilisateur Web	N/A	L'un des navigateurs suivants : ■ Microsoft Internet Explorer 9x, 10 ■ Google Chrome version 17 ou 18 ■ Mozilla Firefox 4.*x* à 15.0 ■ Apple Safari **Remarque :** Si vous utilisez Firefox ou Chrome, désactivez le correcteur orthographique intégré pour éviter des opérations inutiles.	JavaScript activé Adobe Flash Player

Configuration matérielle requise

Le tableau suivant indique la configuration matérielle minimale requise pour chaque composant CA Process Automation.

Composant CA Process Automation	Matériel requis
orchestrateur	■ Classe de serveur exécutant plusieurs UC ou des UC à plusieurs coeurs ■ 8 Go de RAM ■ 40 Go d'espace disque requis ■ Connexion réseau 100 Mbits/s **Remarque :** Une connexion 1000 Mbits/s est recommandée.
Agent	■ Hôte capable d'exécuter un système d'exploitation pris en charge ■ 2 Go de RAM ■ 4 Go d'espace disque ■ Connexion réseau 100 Mbits/s
Serveur de base de données	Consultez les spécifications du fournisseur. Stockage supplémentaire requis pour les bases de données hébergées. **Remarque :** Il est recommandé de réserver un espace disque minimum de 40 Go pour vos bases de données.

Composant CA Process Automation	Matériel requis
CA EEM	Reportez-vous à la documentation CA Embedded Entitlements Manager.
Interface utilisateur Web	Hôte capable d'exécuter un explorateur pris en charge

Remarque : Les configurations sont applicables aussi bien aux machines physiques qu'aux machines virtuelles.

Chapitre 4: Configuration d'un équilibreur de charge pour la mise en cluster d'un orchestrateur

Il est vivement recommandé de remplacer vos équilibreurs de charge Apache par des équilibreurs de charge NGINX. NGINX active la communication simplifiée entre des agents et des orchestrateurs ; Apache prend en charge uniquement la communication désapprouvée.

Si vous prévoyez de mettre en cluster un orchestrateur ultérieurement, configurez un équilibreur de charge avant d'installer l'orchestrateur, puis configurez l'orchestrateur comme node1.

Le processus de haut niveau de NGINX est similaire à celui d'Apache :

1. Installez un équilibreur de charge.
2. Configurez les communications de base.
3. Installez CA Process Automation, y compris les noeuds de cluster.
4. Générez les fichiers de certificat SSL.
5. Configurez les communications sécurisées.

Ce chapitre traite des sujets suivants :

Equilibreur de charge NGINX (page 35)
Conditions requises pour l'équilibreur de charge F5 (page 53)

Equilibreur de charge NGINX

Un *orchestrateur mis en cluster* est un ensemble de noeuds qui s'affiche et agit comme un orchestrateur unique, et qui utilise une bibliothèque partagée. Vous pouvez mettre en cluster un orchestrateur CA Process Automation pour garantir une haute disponibilité, la tolérance aux pannes et la modularité.

Un équilibreur de charge, tel que le serveur HTTP NGINX, est requis pour mettre en cluster un orchestrateur, y compris l'orchestrateur de domaine. Aucun équilibreur de charge ne fait partie de l'installation CA Process Automation. Avant d'installer CA Process Automation, vous devez installer et configurer un équilibreur de charge.

Le mode de communication simplifiée, introduit dans CA Process Automation 4.2, utilise des sockets Web et HTTP pour créer une connexion persistante unilatérale de l'agent vers l'orchestrateur. CA Technologies prend en charge NGINX pour cette nouvelle méthode de communication simplifiée, mais vous pouvez utiliser un autre équilibreur de charge prenant en charge les sockets Web.

Remarque : L'équilibreur de charge Apache ne prend *pas* en charge le mode de communication simplifiée pour les agents. Vous devez donc utiliser NGINX ou un autre équilibreur de charge basé sur des sockets Web pour tirer parti de cette fonctionnalité. Si vous n'utilisez pas la méthode de communication simplifiée et que vous voulez utiliser la méthode de communication héritée, vous pouvez installer l'équilibreur de charge Apache.

Installez l'équilibreur de charge NGINX sur un hôte externe à CA Process Automation pour assurer la compatibilité du système d'exploitation. Pour des informations sur les systèmes d'exploitation pris en charge, consultez la documentation de NGINX.

Un équilibreur de charge est *uniquement* requis pour un orchestrateur dans une configuration en cluster et dans certaines configurations d'authentification unique.

Important : Si vous voulez mettre en cluster un orchestrateur autonome existant, installez et configurez un équilibreur de charge, puis réinstallez l'orchestrateur.

Configuration requise

La configuration requise pour l'utilisation de l'équilibreur de charge NGINX est la suivante.

Installation de NGINX

NGINX est un logiciel de serveur Web libre que vous pouvez télécharger et installer pour votre système d'exploitation. CA Process Automation est certifié avec la version 1.4.2 de NGINX. Suivez les instructions suivantes pour vous familiariser.

Windows

Téléchargez le package NGINX et extrayez les fichiers.

Linux

Procédez comme suit :

1. Téléchargez le package NGINX et extrayez les fichiers.
2. Ouvrez une invite de commande
3. Exécutez la commande suivante pour installer des packages :

```
rpm -ivh nginx-release-rhel-6-0.el6.ngx.noarch.rpm
wget
http://nginx.org/packages/rhel/6/noarch/RPMS/nginx-release-
rhel-6-0.el6.ngx.noarch.rpm
yum install nginx
```

Remarque : Les commandes précédentes concernent Red Hat Enterprise Linux. Sous d'autres versions de Linux, consultez le système d'exploitation et la documentation de NGINX pour obtenir les commandes équivalentes.

Sous Windows et Linux, appelez NGINX à l'aide d'une invite de commande. Accédez à l'emplacement du répertoire NGINX et saisissez :

```
nginx.exe
```

Pour vérifier que NGINX est correctement installé et en cours d'exécution, accédez à l'URL suivante à partir d'un navigateur :

http://*nom_hôte*:80

Copie des modèles de configuration

A l'issue de l'installation de NGINX, extrayez les fichiers modèles à partir du média d'installation de CA Process Automation vers le répertoire d'installation de NGINX.

Procédez comme suit :

1. Accédez au dossier suivant dans le média d'installation CA Process Automation :

   répertoire_installation\DVD1/NginxConfTemplates
2. Extrayez les fichiers de NginxConfig.zip.
3. Accédez au sous-dossier CA Process Automation. Ce dossier inclut les fichiers suivants :

   pam-server.conf

   Utilisé pour la configuration non sécurisée

   secure-pam-server.conf

   Utilisé pour la configuration sécurisée

   pam-rest.conf

   Utilisé pour la configuration de REST

   Ces fichiers sont spécifiques à la configuration de CA Process Automation avec NGINX.
4. Copiez ces trois fichiers et collez-les dans le dossier suivant :

   répertoire_installation_nginx/conf

   Vous pouvez configurer l'équilibreur de charge NGINX.

Communication simple

Les instructions suivantes décrivent la procédure de configuration de la communication simple, non sécurisée pour NGINX sous les systèmes Windows et Linux.

Windows

Procédez comme suit :

1. Accédez au dossier suivant :

   répertoire_installation_nginx/conf

   Ce dossier contient le fichier pam-server.conf.

2. Ouvrez le fichier pam-server.conf.

3. Il contient trois blocs de code qui requièrent des modifications pour chaque noeud que vous ajoutez.

   a. Ajoutez le nom d'hôte node1 dans le bloc **upstream loadbalancer** :
   `server <nom_hôte_node1>:8080 max_fails=3 fail_timeout=3s`

   b. Ajoutez le nom d'hôte du node1 dans le bloc **upstream jettyloadbalancer** :
   `server <nom_hôte_node1>:8080 max_fails=3 fail_timeout=3s`

   c. Ajoutez le nom d'hôte du node1 dans le bloc **Define node1** :
   `serveur <nom d'hôte de l'ordinateur où est installé node1>:<port du serveur jetty> max_fails=3 fail_timeout=3s`

   Remplacez l'espace réservé *Enter node1 hostname here* par une valeur valide. Ne modifiez pas les numéros de port sauf si vous utilisez un port différent pour le noeud CA Process Automation.

   Remarque : Les valeurs valides sont l'adresse IP, le nom de domaine complet ou l'alias de DNS qui pointe vers l'hôte sur lequel vous installez le noeud Orchestrateur de domaine initial. La valeur valide est la même que celle utilisée pour Hôte de serveur lors de l'installation de l'orchestrateur de domaine.

   Répétez ces étapes pour chaque noeud supplémentaire que vous installez.

4. Enregistrez et fermez le fichier pam-server.conf.

5. Ouvrez le fichier *répertoire_installation_nginx*/conf/nginx.conf.

6. Ajoutez l'entrée suivante dans le bloc http à la fin du fichier nginx.conf :

   `include nginx_install_dir/conf/pam-server.conf;`

   Cette entrée lie NGINX avec les changements de configuration appliqués à CA Process Automation dans le fichier pam-server.conf.

7. Enregistrez et fermez le fichier nginx.conf.

   Important : Effectuez les autres étapes *après* l'installation d'au moins un noeud d'orchestrateur. Pour obtenir des instructions, reportez-vous aux sections Installation interactive de l'orchestrateur de domaine (page 93) ou Installation autonome de l'orchestrateur de domaine (page 118).

8. A l'issue de l'installation d'au moins un noeud d'orchestrateur, ouvrez le fichier *répertoire_installation_nginx*/conf/nginx.conf.

9. Supprimez tout bloc de code du serveur, car ils peuvent entrer en conflit avec le serveur identifié dans le fichier pam-server.conf.

Exemple :

```
server {
        listen       80;
        server_name  <nom_hôte_équilibreur_charge>;
location / {
             root   /usr/share/nginx/html;
              index  index.html index.htm;
       }
}
```

10. Enregistrez et fermez le fichier nginx.conf.
11. Arrêtez NGINX. Dans une invite de commande, accédez à l'emplacement du répertoire de NGINX et entrez la commande suivante :

    ```
    nginx –s stop
    ```

12. Redémarrez NGINX.

    Les modifications sont appliquées.

Linux

Procédez comme suit :

1. Accédez au dossier suivant :

   répertoire_installation_nginx/conf

   Ce dossier contient le fichier nginx.conf.

2. Ouvrez le fichier nginx.conf.

3. Pour vérifier l'installation NGINX autonome, indiquez le bloc de serveur comme suit.

```
server {
        listen       80;
        server_name  <nom_hôte_équilibreur_charge>;
location / {
             root   /usr/share/nginx/html;
              index  index.html index.htm;
       }
}
```

4. Enregistrez le fichier, puis fermez l'éditeur.

5. Accédez au dossier suivant :

   répertoire_installation_nginx/conf

   Ce dossier contient le fichier pam-server.conf.

6. Ouvrez le fichier pam-server.conf.

7. Il contient trois blocs de code qui requièrent des modifications pour chaque noeud que vous ajoutez.

   a. Ajoutez le nom d'hôte node1 dans le bloc **upstream loadbalancer** :
   `server <nom_hôte_node1>:8080 max_fails=3 fail_timeout=3s`

   b. Ajoutez le nom d'hôte du node1 dans le bloc **upstream jettyloadbalancer** :
   `server <nom_hôte_node1>:8080 max_fails=3 fail_timeout=3s`

   c. Ajoutez le nom d'hôte du node1 dans le bloc **Define node1** :
   `serveur <nom d'hôte de l'ordinateur où est installé node1>:<port du serveur jetty> max_fails=3 fail_timeout=3s`

   Remplacez l'espace réservé *Enter node1 hostname here* par une valeur valide. Ne modifiez pas les numéros de port sauf si vous utilisez un port différent pour le noeud CA Process Automation.

   Remarque : Les valeurs valides sont l'adresse IP, le nom de domaine complet ou l'alias de DNS qui pointe vers l'hôte sur lequel vous installez le noeud Orchestrateur de domaine initial. La valeur valide est la même que celle utilisée pour Hôte de serveur lors de l'installation de l'orchestrateur de domaine.

   Répétez ces étapes pour chaque noeud supplémentaire que vous installez.

8. Enregistrez et fermez le fichier pam-server.conf.
9. Ouvrez le fichier nginx.conf.
10. Ajoutez l'entrée suivante dans le bloc http à la fin du fichier nginx.conf :

    ```
    include nginx_install_dir/conf/pam-server.conf;
    ```

    Cette entrée lie NGINX avec les changements de configuration appliqués à CA Process Automation dans le fichier pam-server.conf.
11. Supprimez l'entrée suivante :

    ```
    include répertoire_installation_nginx/nginx/conf.d/*.conf;
    ```
12. Enregistrez et fermez le fichier nginx.conf.

    Important : Effectuez les autres étapes *après* l'installation d'au moins un noeud d'orchestrateur. Pour obtenir des instructions, reportez-vous aux sections Installation interactive de l'orchestrateur de domaine (page 93) ou Installation autonome de l'orchestrateur de domaine (page 118).
13. A l'issue de l'installation d'au moins un noeud d'orchestrateur, ouvrez le fichier *répertoire_installation_nginx*/conf/nginx.conf.
14. Supprimez tout bloc de code du serveur, car ils peuvent entrer en conflit avec le serveur identifié dans le fichier pam-server.conf.

    Exemple :

    ```
    server {
            listen       80;
            server_name  <nom_hôte_équilibreur_charge>;
    location / {
                root   /usr/share/nginx/html;
                 index  index.html index.htm;
           }
    }
    ```
15. Enregistrez et fermez le fichier nginx.conf.
16. Arrêtez NGINX. Dans une invite de commande, accédez à l'emplacement du répertoire de NGINX (nginx-1.42) et entrez la commande suivante :

    ```
    nginx –s stop
    ```
17. Redémarrez NGINX.

    Les modifications sont appliquées.

Communication sécurisée

Les instructions suivantes décrivent la procédure de configuration de la communication sécurisée pour NGINX sous les systèmes Windows et Linux. La communication sécurisée est différente de la communication simple en ce qu'elle requiert l'utilisation de certificats et des fichiers de clé.

Windows

La communication sécurisée pour NGINX requiert des certificats SSL (fichiers c2okey2.pem et c2ocert.pem). Avant de démarrer cette procédure, veillez à générer ces fichiers (page 50).

Procédez comme suit :

1. Accédez au dossier suivant :

   répertoire_installation_nginx/conf

   Ce dossier contient le fichier secure-pam-server.conf.

2. Ouvrez le fichier secure-pam-server.conf.

3. Il contient trois blocs de code qui requièrent des modifications pour chaque noeud que vous ajoutez. Modifiez les blocs en fonction de vos mesures de sécurité.

   a. Ajoutez le nom d'hôte node1 dans le bloc **upstream loadbalancer** :
   `server <nom_hôte_node_1 ici>:8443 max_fails=3 fail_timeout=3s`

   b. Ajoutez le nom d'hôte du node1 dans le bloc **upstream jettyloadbalancer** :
   `server <nom_hôte_node_1 ici>:8443 max_fails=3 fail_timeout=3s`

   c. Ajoutez le nom d'hôte du node1 dans le bloc **Define node1** :
   `serveur <nom d'hôte de l'ordinateur où est installé node1>:<port du serveur jetty> max_fails=3 fail_timeout=3s`

   Remplacez l'espace réservé *Enter node1 hostname here* par une valeur valide. Ne modifiez pas les numéros de port sauf si vous utilisez un port différent pour le noeud CA Process Automation.

   Remarque : Les valeurs valides sont l'adresse IP, le nom de domaine complet ou l'alias de DNS qui pointe vers l'hôte sur lequel vous installez le noeud Orchestrateur de domaine initial. La valeur valide est la même que celle utilisée pour Hôte de serveur lors de l'installation de l'orchestrateur de domaine.

   Répétez ces étapes pour chaque noeud supplémentaire que vous installez.

4. Mettez à jour les lignes suivantes en spécifiant l'emplacement des fichiers c2ocert.pem et c2okey2.pem (dans le répertoire emplacement_installation_nginx/conf).

   ```
   ssl_certificate      <emplacement_certificat/c2ocert.pem>;
   ssl_certificate_key  <emplacement_certificat/c2okey2.pem>;
   ```

   Exemple :

   ```
   ssl_certificate
   <répertoire_installation_nginx\conf\c2ocert.pem>;
   ```

5. Enregistrez et fermez le fichier secure-pam-server.conf.

6. Ouvrez le fichier nginx.conf.

7. Ajoutez l'entrée suivante dans le bloc http à la fin du fichier nginx.conf :
   `include` *`répertoire_installation_nginx`*`/conf/secure-pam-server.conf;`

   Cette entrée lie NGINX avec les changements de configuration appliqués à CA Process Automation dans le fichier secure-pam-server.conf.

8. Enregistrez et fermez le fichier nginx.conf.

   Important : Effectuez les autres étapes *après* l'installation d'au moins un noeud d'orchestrateur. Pour obtenir des instructions, reportez-vous aux sections Installation interactive de l'orchestrateur de domaine (page 93) ou Installation autonome de l'orchestrateur de domaine (page 118).

9. A l'issue de l'installation d'au moins un noeud d'orchestrateur, ouvrez le fichier *répertoire_installation_nginx*/conf/nginx.conf.

10. Supprimez tous les blocs de code du serveur, car ils peuvent entrer en conflit avec le serveur identifié dans le fichier secure-pam-server.

    Exemple :

    ```
    server {
            listen       80;
            server_name  <nom_hôte_équilibreur_charge>;
    location / {
                 root   /usr/share/nginx/html;
                  index  index.html index.htm;
           }
    }
    ```

11. Enregistrez et fermez le fichier nginx.conf.

12. Arrêtez NGINX. Dans une invite de commande, accédez à l'emplacement du répertoire de NGINX (nginx-1.42) et entrez la commande suivante :

    ```
    nginx –s stop
    ```

13. Redémarrez NGINX.

    Les modifications sont appliquées.

Linux

La communication sécurisée pour NGINX requiert des certificats SSL (fichiers c2okey2.pem et c2ocert.pem). Avant de démarrer cette procédure, veillez à générer ces fichiers (page 50).

Procédez comme suit :

1. Accédez au dossier suivant :

   répertoire_installation_nginx/conf

   Ce dossier contient le fichier nginx.conf.

2. Ouvrez le fichier nginx.conf.

3. Pour vérifier l'installation NGINX autonome, indiquez le bloc de serveur comme suit.

```
server {
        listen       80;
        server_name  <nom_hôte_équilibreur_charge>;
location / {
             root   /usr/share/nginx/html;
              index  index.html index.htm;
       }
}
```

4. Enregistrez le fichier, puis fermez l'éditeur.

5. Accédez au dossier suivant :

   répertoire_installation_nginx/conf

   Ce dossier contient le fichier secure-pam-server.conf.

6. Ouvrez le fichier secure-pam-server.conf.

7. Il contient trois blocs de code qui requièrent des modifications pour chaque noeud que vous ajoutez. Modifiez les blocs en fonction de vos mesures de sécurité.

   a. Ajoutez le nom d'hôte node1 dans le bloc **upstream loadbalancer** :
   `server <nom_hôte_node_1 ici>:8443 max_fails=3 fail_timeout=3s`

   b. Ajoutez le nom d'hôte du node1 dans le bloc **upstream jettyloadbalancer** :
   `server <nom_hôte_node_1 ici>:8443 max_fails=3 fail_timeout=3s`

   c. Ajoutez le nom d'hôte du node1 dans le bloc **Define node1** :
   `serveur <nom d'hôte de l'ordinateur où est installé node1>:<port du serveur jetty> max_fails=3 fail_timeout=3s`

   Remplacez l'espace réservé *Enter node1 hostname here* par une valeur valide. Ne modifiez pas les numéros de port sauf si vous utilisez un port différent pour le noeud CA Process Automation.

Remarque : Les valeurs valides sont l'adresse IP, le nom de domaine complet ou l'alias de DNS qui pointe vers l'hôte sur lequel vous installez le noeud Orchestrateur de domaine initial. La valeur valide est la même que celle utilisée pour Hôte de serveur lors de l'installation de l'orchestrateur de domaine.

Répétez ces étapes pour chaque noeud supplémentaire que vous installez.

8. Mettez à jour les lignes suivantes en spécifiant l'emplacement des fichiers c2ocert.pem et c2okey2.pem (dans le répertoire emplacement_installation_nginx/conf).

```
ssl_certificate      <emplacement_certificat/c2ocert.pem>;
ssl_certificate_key  <emplacement_certificat/c2okey2.pem>;
```

Exemple :

```
ssl_certificate
<répertoire_installation_nginx\conf\c2ocert.pem>;
```

9. Enregistrez et fermez le fichier secure-pam-server.conf.
10. Ouvrez le fichier nginx.conf.
11. Ajoutez l'entrée suivante dans le bloc http à la fin du fichier nginx.conf :

    `include` *`nginx_install_dir`*`/conf/pam-server.conf;`

    Cette entrée lie NGINX avec les changements de configuration appliqués à CA Process Automation dans le fichier secure-pam-server.conf.
12. Supprimez l'entrée suivante :

    `include` *`répertoire_installation_nginx`*`/nginx/conf.d/*.conf;`
13. Enregistrez et fermez le fichier nginx.conf.

    Important : Effectuez les autres étapes *après* l'installation d'au moins un noeud d'orchestrateur. Pour obtenir des instructions, reportez-vous aux sections Installation interactive de l'orchestrateur de domaine (page 93) ou Installation autonome de l'orchestrateur de domaine (page 118).
14. A l'issue de l'installation d'au moins un noeud d'orchestrateur, ouvrez le fichier *répertoire_installation_nginx*/conf/nginx.conf.
15. Supprimez tous les blocs de code du serveur, car ils peuvent entrer en conflit avec le serveur identifié dans le fichier secure-pam-server.conf.

    Exemple :

    ```
    server {
            listen       80;
            server_name  <nom_hôte_équilibreur_charge>;
    location / {
                root   /usr/share/nginx/html;
                 index  index.html index.htm;
           }
    }
    ```
16. Enregistrez et fermez le fichier nginx.conf.
17. Arrêtez NGINX. Dans une invite de commande, accédez à l'emplacement du répertoire de NGINX (nginx-1.42) et entrez la commande suivante :

    `nginx –s stop`
18. Redémarrez NGINX.

    Les modifications sont appliquées.

Configuration d'REST

CA Process Automation fournit l'option permettant de configurer un équilibreur de charge NGINX pour l'API Catalyst RESTful. Les instructions suivantes décrivent la procédure de configuration de l'équilibreur de charge NGINX pour utiliser REST pour la communication simple et sécurisée sous des systèmes Windows et Linux.

Communication simple

Procédez comme suit :

1. Accédez au dossier suivant :

   répertoire_installation_nginx/conf

   Ce dossier contient le fichier pam-rest.conf.

2. Ouvrez le fichier pam-rest.conf.

3. Modifiez le bloc de code suivant :

   ```
   HTTP
   upstream ucfcluster  {
     server <nom_hôte_node1 ici>:7000 max_fails=3 fail_timeout=5s;
     server <nom_hôte_node2 ici>:7000 max_fails=3 fail_timeout=5s;
   }
   ```

   Remplacez l'espace réservé *Enter node1 hostname here* par une valeur valide. Ne modifiez pas les numéros de port sauf si vous utilisez un port différent pour le noeud CA Process Automation.

   Répétez ces étapes pour chaque noeud supplémentaire que vous installez.

4. Enregistrez et fermez le fichier pam-rest.conf.

5. Ouvrez le fichier nginx.conf.

6. Ajoutez l'entrée suivante dans le bloc http à la fin du fichier nginx.conf :
   `include` *répertoire_installation_nginx*`/conf/pam-rest.conf;`

   Cette entrée lie NGINX avec les changements de configuration appliqués à CA Process Automation dans le fichier pam-rest.conf.

7. Enregistrez et fermez le fichier nginx.conf.

   Important : Effectuez les autres étapes *après* l'installation d'au moins un noeud d'orchestrateur. Pour obtenir des instructions, reportez-vous aux sections Installation interactive de l'orchestrateur de domaine (page 93) ou Installation autonome de l'orchestrateur de domaine (page 118).

8. A l'issue de l'installation d'au moins un noeud d'orchestrateur, ouvrez le fichier *répertoire_installation_nginx*/conf/nginx.conf.

9. Enregistrez et fermez le fichier nginx.conf.

10. Arrêtez NGINX. Dans une invite de commande, accédez à l'emplacement du répertoire de NGINX (nginx-1.42) et entrez la commande suivante :

    ```
    nginx –s stop
    ```

11. Redémarrez NGINX.

    Les modifications sont appliquées.

Communication sécurisée

Les fichiers de certificat SSL sont requis pour la communication sécurisée avec REST. Avant de démarrer cette procédure, veillez à générer ces fichiers (page 50).

Procédez comme suit :

1. Accédez au dossier suivant :

   répertoire_installation_nginx/conf

   Ce dossier contient le fichier pam-rest.conf.

2. Ouvrez le fichier pam-rest.conf.

3. Modifiez le bloc de code suivant :

   ```
   ## HTTPS
   upstream sslcluster  {
     server <nom_hôte_node1 ici>:7443 max_fails=3 fail_timeout=5s;
     server <nom_hôte_node2 ici>:7443 max_fails=3 fail_timeout=5s;
   }
   ```

   Remplacez l'espace réservé *Enter node1 hostname here* par une valeur valide. Ne modifiez pas les numéros de port sauf si vous utilisez un port différent pour le noeud CA Process Automation.

   Répétez ces étapes pour chaque noeud supplémentaire que vous installez.

4. Mettez à jour les lignes suivantes en spécifiant l'emplacement des fichiers c2ocert.pem et c2okey2.pem (dans le répertoire emplacement_installation_nginx/conf).

   ```
   ssl_certificate      <emplacement_certificat/c2ocert.pem>;
   ssl_certificate_key  <emplacement_certificat/c2okey2.pem>;
   ```

   Exemple :

   ```
   ssl_certificate
   <répertoire_installation_nginx\conf\c2ocert.pem>;
   ```

5. Enregistrez et fermez le fichier pam-rest.conf.

6. Ouvrez le fichier nginx.conf.

7. Ajoutez l'entrée suivante dans le bloc http à la fin du fichier nginx.conf :
   `include répertoire_installation_nginx/conf/pam-rest.conf;`

   Cette entrée lie NGINX avec les changements de configuration appliqués à CA Process Automation dans le fichier pam-rest.conf.

8. Enregistrez et fermez le fichier nginx.conf.

   Important : Effectuez les autres étapes *après* l'installation d'au moins un noeud d'orchestrateur. Pour obtenir des instructions, reportez-vous aux sections Installation interactive de l'orchestrateur de domaine (page 93) ou Installation autonome de l'orchestrateur de domaine (page 118).

9. A l'issue de l'installation d'au moins un noeud d'orchestrateur, ouvrez le fichier *répertoire_installation_nginx*/conf/nginx.conf.

10. Enregistrez et fermez le fichier nginx.conf.

11. Arrêtez NGINX. Dans une invite de commande, accédez à l'emplacement du répertoire de NGINX (nginx-1.42) et entrez la commande suivante :

    `nginx –s stop`

12. Redémarrez NGINX.

    Les modifications sont appliquées.

Génération de fichiers de certificat SSL

Les certificats SSL doivent être générés *après* l'installation de CA Process Automation, mais *avant* la configuration de la communication sécurisée pour votre équilibreur de charge. Les certificats SSL ne sont pas requis si vous voulez utiliser la communication simple, non sécurisée pour votre équilibreur de charge.

Une fois générés, l'emplacement des fichiers de certificat doit être identifié lors de la configuration de l'équilibreur de charge pour la communication sécurisée.

Procédez comme suit :

1. Téléchargez et installez OpenSSL à partir d'un fournisseur tiers.

   Remarque : Assurez-vous que le kit de développement Java (JDK) est installé sur l'hôte sur lequel vous installez OpenSSL.

2. A l'issue de l'installation de CA Process Automation en mode de cluster (avec au moins un noeud), l'assistant d'installation de CA Process Automation génère le fichier c2okeystore à l'emplacement suivant :

   ```
   \server_location\c2o\.config
   ```

   Copiez le fichier c2okeystore et collez-le dans le répertoire suivant :

   ```
   \jdk_location\bin
   ```

   Vous pouvez exécuter les commandes localement à partir de cet emplacement.

3. Utilisez l'utilitaire Keytool du JDK pour importer le magasin de clés au format pksc12, en procédant comme suit :

   a. Accédez au répertoire jdk_location\bin et exécutez la commande suivante :

      ```
      keytool -importkeystore -srckeystore c2okeystore
      -srcstoretype jks -destkeystore c2okeystore.p12
      -deststoretype pkcs12
      ```

      La console vous invite à saisir le mot de passe du magasin de clés de destination.

      Remarque : Le fichier OasisConfig.properties contient le mot de passe du magasin de clés. Recherchez le fichier dans ce répertoire : `\server_location\c2o\.config\`

      Ouvrez le fichier et copiez le mot de passe. La valeur se trouve à côté de l'entrée KEYSTOREID=.

      Par exemple : KEYSTOREID=723e1830-a98c-49a1-8f16-a0794c872835. Le mot de passe est 723e1830-a98c-49a1-8f16-a0794c872835.

   b. Collez le mot de passe dans l'invite de mot de passe du magasin de clés de destination dans votre console ouverte.

   c. Lorsque vous y êtes invité, ressaisissez le mot de passe.

   d. A l'invite de mot de passe de la clé de source, entrez le mot de passe à nouveau.

      Un fichier c2okeystore.p12 est généré dans le répertoire \jdk_location\bin.

   e. Vous devez convertir le magasin de clés au format p12 en fichiers de clé et de certificat au format PEM. Pour cela, exécutez la commande openssl à l'emplacement du répertoire \jdk_location\bin :

      ```
      openssl pkcs12 -nocerts -in c2okeystore.p12 -out c2okey.pem
      ```

   f. Lorsque l'invite Import Password (Importer un mot de passe) s'ouvre, entrez le mot de passe du magasin de clés.

g. Lorsque l'invite Phrase secrète s'ouvre, entrez une expression.

h. Ressaisissez la phrase secrète PEM.

i. A l'emplacement du répertoire \jdk_location\bin, exécutez la commande suivante :
```
openssl pkcs12 -clcerts -in c2okeystore.p12 -out c2ocert.pem
```

j. Lorsque l'invite Import Password (Importer un mot de passe) s'ouvre, entrez le mot de passe du magasin de clés.

k. Lorsque l'invite Phrase secrète s'ouvre, saisissez l'expression créée à l'étape g.

l. Ressaisissez la phrase secrète PEM.

m. A l'emplacement du répertoire \jdk_location\bin, exécutez la commande suivante :
```
openssl rsa -in c2okey.pem -out c2okey2.pem
```

n. Lorsque l'invite Phrase secrète s'ouvre, saisissez l'expression créée à l'étape g.

o. Ressaisissez la phrase secrète PEM.

p. Copiez les fichiers c2okey2.pem et c2ocert.pem dans le répertoire \conf de votre équilibreur de charge.

Remarque : Effectuez une sauvegarde de ces fichiers.

Conditions requises pour l'équilibreur de charge F5

Chaque orchestrateur mis en cluster requiert un équilibrage de la charge. Si vous disposez d'un équilibreur de charge F5, vous pouvez l'utiliser pour équilibrer le traitement des demandes d'opérateur ou de services Web sur les noeuds de cluster de l'orchestrateur cible.

Avant d'installer le premier noeud d'un orchestrateur de domaine mis en cluster ou un autre orchestrateur mis en cluster, configurez l'équilibreur de charge F5.

En premier lieu, rassemblez les informations suivantes :

- Identité des hôtes ou des serveurs virtuels sur lesquels les noeuds d'orchestrateur seront déployés
- Informations d'identification pour la connexion à l'interface F5.

Vous devez configurer les éléments F5 suivants de manière à ce qu'ils fonctionnent avec CA Process Automation.

1. Création d'un noeud F5 pour chaque noeud de cluster (page 54)

   Dans CA Process Automation, un noeud est un hôte ou un serveur virtuel sur lequel un noeud de cluster d'orchestrateur est installé (ou peut être ultérieurement installé).

2. Création d'un pool F5 pour chaque cluster CA Process Automation (page 55)

   Dans CA Process Automation, chaque pool inclut les noeuds de cluster d'orchestrateur qui appartiennent au même orchestrateur mis en cluster.

3. Création d'une iRule F5 pour CA Process Automation (page 56)

   Dans CA Process Automation, une iRule achemine les demandes d'opérateur pour lesquelles le point de contact d'un orchestrateur mis en cluster est la cible.

4. Création d'un serveur virtuel F5 pour CA Process Automation (page 59)

   F5 peut inclure plusieurs serveurs virtuels. CA Process Automation est configuré comme l'un des serveurs virtuels.

5. Configurez F5 pour utiliser la communication simplifiée HTTPS (page 61).
6. Préparation de l'équilibreur de charge F5 pour la vérification de la communication (page 63).
7. Activez les sessions rémanentes sur l'équilibreur de charge F5. Les sessions rémanentes doivent être activées sur l'équilibreur de charge F5 pour qu'il puisse fonctionner avec un cluster CA Process Automation.

Création d'un noeud F5 pour chaque noeud de cluster

Cette opération permet de configurer les noeuds que vous envisagez d'ajouter à un orchestrateur mis en cluster, plutôt que de configurer les noeuds de cluster une fois qu'ils ont été ajoutés dans CA Process Automation.

Procédez comme suit :

1. Connectez-vous à l'application F5.
2. Sélectionnez l'onglet Main, cliquez sur Local Traffic, puis sur Nodes.

   La liste Node List affiche les détails suivants pour chaque noeud de réseau défini sur F5 : le statut, l'adresse IP, la partition et le nom d'hôte.
3. Cliquez sur Créer.

   La page New Node s'affiche.
4. Fournissez toutes les informations nécessaires dans la section General Properties.

   Address

   Indique l'adresse IP du nouveau noeud.

   Name

   Spécifie le nom d'hôte de l'adresse IP associée.
5. Fournissez toutes les informations nécessaires dans la section Configuration.

   Health Monitors

   Spécifie le moniteur d'intégrité de ce noeud. S'il n'est pas configuré, sélectionnez None.

   Valeur par défaut : Node Default

   Ratio

   Spécifie la valeur pondérée à affecter au noeud. Si la capacité est identique pour tous les noeuds qui appartiennent au même cluster, entrez la valeur de Ratio 1 pour chaque noeud.

   Connection Limit

   Spécifie le nombre maximum de connexions que ce noeud peut gérer.
6. Cliquez sur Finished.

   Le noeud ajouté apparaît dans la liste Node List.

Création de deux pools F5 pour chaque cluster CA Process Automation

Créez deux pools F5 pour chaque cluster CA Process Automation. Pour chaque pool F5 que vous créez, ajoutez les noeuds qui appartiennent au cluster associé.

Par exemple, créez deux pools comme illustré dans les exemples suivants :

- Le pool PAMPOOL nommé PAMSRVPOOL, dans lequel les membres utilisent le port 8080 (de base) ou le port 8443 (sécurisé). Ce pool est utilisé pour toutes les communications.
- Le pool PAMWSPOOL nommé PAMJETTYPOOL, dans lequel les membres utilisent le port 80 (de base) ou le port 443 (sécurisé). Ce pool prend en charge des agents configurés pour la communication simplifiée, qui utilisent des sockets Web.

Procédez comme suit :

1. Connectez-vous à l'application F5.
2. Sélectionnez l'onglet Main, cliquez sur Local Traffic, puis sur Pools.

   La liste Pool List est vide si vous configurez des pools pour la première fois. La liste Pool List affiche les informations suivantes pour chaque pool : statut, nom du pool, partition et nombre de membres présents dans le pool.
3. Cliquez sur Créer.

   La page New Pool s'affiche.
4. Fournissez toutes les informations nécessaires dans la section Configuration.
   a. Dans la liste déroulante, sélectionnez Simple.
   b. Attribuez un nom au nouveau pool.
   c. Dans la liste des moniteurs d'intégrité disponibles, sélectionnez http et déplacez-le dans la liste des moniteurs actifs.
5. Dans la liste déroulante Load Balancing Method, sélectionnez Round Robin.
6. Dans la liste déroulante Priority Group Activation, sélectionnez Disabled.
7. Ajoutez chaque noeud au nouveau pool F5 en procédant comme suit :
   a. Sélectionnez Node List, puisque que vous ajoutez un noeud qui est déjà défini.
   b. Sélectionnez l'adresse IP (nom d'hôte) dans la liste déroulante Address qui identifie le noeud à ajouter à ce pool F5.
   c. Entrez l'une des valeurs suivantes pour le port de service en fonction du niveau de sécurité de la communication (simple ou sécurisée) et pour le type de communication (désapprouvée ou simplifiée) :

      Communication simple (non sécurisée) et désapprouvée

      8080

      Communication simple (non sécurisée) et simplifiée

80 ; sélectionnez HTTP ; 80 est automatiquement rempli dans le champ Service Port.

Communication sécurisée et désapprouvée

8443

Communication sécurisée et simplifiée

443 ; sélectionnez HTTPS ; 443 est automatiquement rempli dans le champ Service Port.

d. Cliquez sur Ajouter.

Les détails que vous avez ajoutés pour ce noeud s'affichent dans la liste New Members.

8. Cliquez sur Terminé.

Le nouveau pool est ajouté à la liste F5 Pool List.

Création d'une iRule F5 pour CA Process Automation

Une iRule achemine les demandes d'opérateur pour lesquelles le point de contact d'un orchestrateur mis en cluster est la cible. F5 crée une URL à partir de ces informations et l'utilise comme destination de point de contact. Pour créer une iRule F5 pour CA Process Automation, copiez la définition de l'iRule fournie dans la zone de texte Description. Définissez ensuite les valeurs pour la variable *MyPool*.

Remarque : Les iRule équivalent aux fichiers uriworkermap.properties dans Apache. Une iRule identifie un noeud de cluster d'orchestrateur pour une demande qui cible le point de contact d'un orchestrateur mis en cluster. La décision dépend de l'URL.

Procédez comme suit :

1. Connectez-vous à l'application F5.
2. Sélectionnez l'onglet Main, cliquez sur Local Traffic, puis sur iRules.

   La liste iRules List est vide si vous configurez des iRules pour la première fois. La liste iRules List affiche les informations suivantes pour chaque iRule : le nom de l'iRule et la partition.
3. Cliquez sur Créer.

   La page New iRule s'affiche.

4. Fournissez toutes les informations nécessaires dans la section Properties.

   Nom

   Spécifie le nom de l'iRule.

   Définition

   Spécifie la définition d'iRule. Copiez le texte de la définition d'iRule (page 58) dans cette zone de texte.

   Remarque : Le langage de programmation utilisé pour les iRules est Tcl (Tool Command Language).

   Extend Text Area

   Permet de développer la zone de texte Definition à sa taille maximum.

   Option activée : développe la zone de texte à sa taille maximum.

   Option désactivée : affiche la zone de texte dans sa taille normale.

   Wrap Text (Retour automatique à la ligne)

   Permet d'activer le retour automatique à la ligne pour que le texte soit ajusté à la zone Definition et qu'aucune barre de défilement horizontale ne soit affichée.

   Option activée : active le retour automatique à la ligne lorsque le texte s'étend au-delà de la portion affichable de la zone Definition.

   Option désactivée : le texte est présenté tel qu'il est saisi, avec une barre de défilement horizontale, si nécessaire.

5. Cliquez sur Terminé.

   L'iRule que vous entrez s'affiche dans la liste iRule List.

Définition d'iRule

Dans la zone de texte Definition pour votre nouvelle iRule, saisissez la définition suivante. Adaptez les valeurs des instructions de définition si nécessaire.

- Définissez la variable BasicPool sur des valeurs spécifiques au pool actuel avec le port 8080 pour les communications simples (non sécurisées).
- Définissez les adresses IP de NODE1 et NODE2 sur les valeurs des serveurs présents dans le pool PAMWSPOOL.
- Utilisez la définition WSPORT 80 pour HTTP ou la définition WSPORT 443 pour utiliser le port sécurisé (HTTPS) pour les communications simplifiées.

```
où HTTP_REQUEST {
set PAMPOOL "PAMSRVRPOOL"
set PAMWSPOOL "PAMJETTYPOOL"
set NODE1 "10.130.5.146"
set NODE2 "10.130.5.147"
set WSPORT "80"
   switch -glob [HTTP::uri] {
      "/jmx-console*" { pool $PAMPOOL }
      "/web-console*" { pool $PAMPOOL }
      "/c2orepository/*" { pool $PAMPOOL }
      "/c2orepository/oasisHelp*" { pool $PAMPOOL }
      "/c2orepository/htmlFile/aboutUs/*" { pool $PAMPOOL }
      "/c2orepository/htmlFile/language/*" { pool $PAMPOOL }
      "/c2orepository/htmlFile/installation/*" { pool $PAMPOOL }
      "/c2orepository/media*" { pool $PAMPOOL }
      "/c2orepository/thirdParty*" { pool $PAMPOOL }
      "/c2orepository/MainInstallerConfiguration.properties" {
      pool $PAMPOOL }
      "/itpam*" { pool $PAMPOOL }
      "/itpam/ServerConfigurationRequestServlet" { pool $PAMPOOL }
      "/itpam/MirroringRequestProcessor*" { pool $PAMPOOL }
      "/itpam/AgentConfigurationRequestServlet" { pool $PAMPOOL }
      "/itpam/StartAgent*" { pool $PAMPOOL }
      "/itpam/OasisPrimary" { pool $PAMPOOL }
      "/itpam/JNLPRequestProcessor*" { pool $PAMPOOL }
      "/itpam/JNLPRequestProcessor/installation" { pool $PAMPOOL }
      "/itpam/clientproxy/c2oresourceaction" { pool $PAMPOOL }
      "/itpam/clientproxy/c2oreportaction" { pool $PAMPOOL }
      "/mirroringrepository*" { pool $PAMPOOL }
      "/birt/*" { pool $PAMPOOL }
      default { pool $PAMPOOL }
      "/ws/node1" { pool $PAMWSPOOL member $NODE1 $WSPORT }
        "/ws/node1/*" { pool $PAMWSPOOL member $NODE1 $WSPORT }
      "/ws/node2" { pool $PAMWSPOOL member $NODE2 $WSPORT }
        "/ws/node2/*" { pool $PAMWSPOOL member $NODE2 $WSPORT }
      "/*" { pool $PAMWSPOOL }
   }
```

```
}
```

Création d'un serveur virtuel F5 pour CA Process Automation

Vous pouvez créer un serveur virtuel F5.

Procédez comme suit :

1. Connectez-vous à l'application F5.
2. Sélectionnez l'onglet Main, cliquez sur Local Traffic, puis sur Virtual Servers.

   La liste Virtual Servers List affiche les informations suivantes pour chaque serveur virtuel : statut, nom, partition, adresse IP de destination, port de service, type et un lien Edit (Modifier) pour les ressources.
3. Cliquez sur Créer.

   La page New Virtual Server s'affiche.
4. Fournissez toutes les informations nécessaires dans la section General Properties.

   Nom

   Spécifie le nom du serveur virtuel, par exemple, PAMLB.

   Destination Type

   Spécifie l'hôte pour une adresse IP unique.

   Destination Address

   Spécifie l'adresse IP du serveur virtuel, par exemple, 10.130.5.149.

   Service Port

   Spécifie le port associé au serveur virtuel, par exemple, 80 pour les connexions HTTP ou 443 pour les connexions HTTPS.

   Etat

   Spécifie si le serveur virtuel est disponible pour l'équilibrage de la charge. Spécifiez Enabled (Activé).

5. Fournissez toutes les informations nécessaires dans la section Configuration. Acceptez toutes les valeurs par défaut, sauf celle du champ HTTP Profile.

   Mode

   Spécifie le type de serveur virtuel. Standard correspond à un serveur virtuel qui dirige l'ensemble du trafic vers le pool que vous avez défini comme pool d'équilibrage de la charge par défaut.

   Valeur par défaut : Standard

   HTTP Profile

   Spécifie le profil HTTP à utiliser pour la gestion gérer du trafic HTTP. Sélectionnez http.

6. Entrez toutes les informations requises dans la section Ressources.

   iRules

   Spécifie les iRules à activer pour ce serveur virtuel. Sélectionnez le script iRules que vous avez créé pour l'orchestrateur mis en cluster.

   Incluez l'iRule que vous avez créé pour le pool par défaut.

   Default Pool

   Spécifie le nom du pool vers lequel le serveur virtuel route le trafic. Spécifiez le pool CA Process Automation en tant que pool par défaut.

   Default Persistence Profile

   Spécifie le profil de persistance pour ce serveur virtuel, source_addr, par exemple.

   Fallback Persistence Profile

   Spécifie le profil de persistance que ce serveur virtuel utilise lorsque vous ne pouvez pas utiliser le profil de persistance par défaut, dest_addr, par exemple.

7. Cliquez sur Terminé.

Configuration de F5 pour utiliser la communication simplifiée HTTPS

La communication SSL dans F5 requiert un fichier de certificat et un fichier de clé. La communication simplifiée peut uniquement utiliser des certificats générés par l'outil keytool et copiés dans le magasin de clés CA Process Automation.

Procédez comme suit :

1. Générez des fichiers de certificat SSL (page 50).
2. Chargez un certificat SSL et une clé.
   a. Connectez-vous à l'application F5.
   b. Cliquez sur Local Traffic, SSL Certificates, Import.
   c. Importez la clé : sélectionnez Clé comme type d'importation, saisissez le nom de la clé, cliquez sur Parcourir et accédez à l'emplacement du fichier de clé, puis cliquez sur Importer.

      user-specified-location/c2okey2.pem

   d. Cliquez sur Local Traffic, SSL Certificates, Import.
   e. Importez le certificat : sélectionnez Certificat comme type d'importation, saisissez le nom du certificat, cliquez sur Parcourir et accédez à l'emplacement du fichier de certificat, puis cliquez sur Importer.

      user-specified-location/c2ocert2.pem

3. Créez le profil Client.
   a. Cliquez sur Local Traffic, Profils, SSL, Client.
   b. Cliquez sur Créer.
   c. Entrez un nom dans le champ Nom. Acceptez la valeur par défaut pour le profil parent : clientssl.
   d. Sélectionnez Avancé pour la configuration.
   e. Sur la partie droite, sélectionnez les champs Certificat, Clé et Phrase secrète pour les rendre modifiables.
   f. Dans la liste déroulante Certificat, sélectionnez le certificat c2ocert2.pem importé lors de l'étape précédente.
   g. Dans la liste déroulante Clé, sélectionnez la clé c2ocert2.pem importée lors de l'étape précédente.
   h. Dans les champs Phrase secrète et Confirmer la phrase secrète, saisissez l'expression clé utilisée pour générer les fichiers de certificat.
   i. Cliquez sur Terminé.

4. Créez le profil Serveur.
   a. Cliquez sur Local Traffic, Profiles, SSL, Server.
   b. Cliquez sur Créer.
   c. Entrez un nom dans le champ Nom. Acceptez la valeur par défaut pour le profil serveur : serverssl.
   d. Sélectionnez Avancé pour la configuration.
   e. Sur la partie droite, sélectionnez les champs Certificat, Clé et Phrase secrète pour les rendre modifiables.
   f. Dans la liste déroulante Certificat, sélectionnez le certificat c2ocert2.pem importé lors de l'étape précédente.
   g. Dans la liste déroulante Clé, sélectionnez la clé c2ocert2.pem importée lors de l'étape précédente.
   h. Dans les champs Phrase secrète et Confirmer la phrase secrète, saisissez l'expression clé utilisée pour générer les fichiers de certificat.
   i. Cliquez sur Terminé.
5. Liez les profils client et serveur au serveur virtuel F5.
   a. Cliquez sur Local Traffic, Virtual Servers, Virtual Server List.
   b. Sélectionnez le serveur virtuel pour CA Process Automation, par exemple : pamlib.

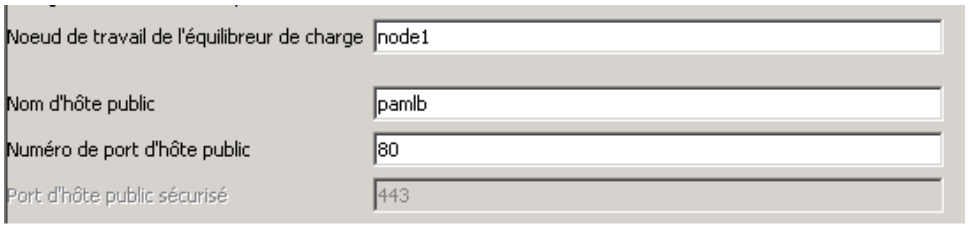
      Notez que le port de service affiche 443 et HTTPS.
   c. Pour SSL Profile, sélectionnez clientssl (valeur par défaut utilisée pour le profil parent dans les deux dernières étapes).
   d. Pour SSL Profile (serveur), sélectionnez serverssl.
   e. Cliquez sur Terminé.

Comparaison des paramètres de port pour HTTPS et HTTP

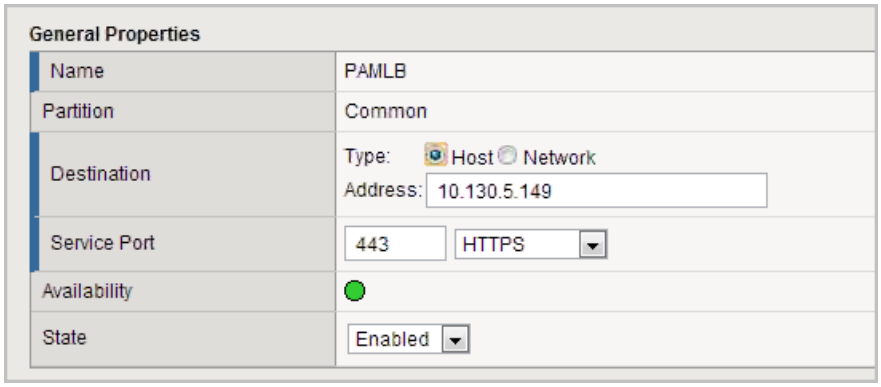
	HTTPS (sécurisé)	HTTP (Simple)
Service Port	443	80
Membres de noeud ajoutés au pool	8443	8080
iRule qui référence le port de socket Web	443	80

Préparation de l'équilibreur de charge F5 pour la vérification de la communication (exemple)

Le processus d'installation d'orchestrateur affiche une page de configuration dans laquelle vous pouvez configurer un équilibreur de charge :



Lors de l'installation de CA Process Automation, entrez le nom d'hôte que vous définissez dans F5 dans le champ Nom d'hôte public. Pour confirmer que CA Process Automation peut communiquer avec l'hôte spécifié dans Nom d'hôte public, le processus d'installation de CA Process Automation soumet une demande HTTP GET à la cible que vous spécifiez. Ce nom d'hôte est mappé vers l'adresse IP privée du serveur virtuel que F5 alloue (une adresse IP qui ne fait pas partie du réseau CA Process Automation local), ce qui peut poser problème. Dans l'exemple suivant, 10.130.5.149 est une adresse IP qui fait partie du réseau F5, mais pas du réseau CA Process Automation.



Si aucune solution n'est fournie, une erreur similaire à l'erreur suivante se produit :

```
java.net.UnknownHostException:pamlb
```

Pour permettre la validation des communications, créez une entrée dans le fichier d'hôtes qui mappe l'entrée du champ Nom d'hôte public vers une adresse IP d'un serveur qui peut répondre à cette demande.

Par exemple, créez une entrée de fichier d'hôtes qui mappe l'entrée du champ Nom d'hôte public vers l'adresse IP d'un serveur dans le réseau CA Process Automation comprenant un équilibreur de charge Apache.

```
xxx.xxx.xxx.xxx      pamlb
```

Une fois que le programme d'installation a dépassé la page de l'équilibreur de charge, supprimez cette ligne du fichier d'hôtes.

Remarque : De même, vous pouvez configurer F5 pour que l'adresse IP allouée puisse accepter la demande d'ouverture de flux HTTP émanant du processus d'installation de l'orchestrateur CA Process Automation. Pour plus d'informations, reportez-vous à la documentation de l'équilibreur de charge F5.

Informations complémentaires :

Ports utilisés par l'équilibreur de charge (page 231)

Chapitre 5: Installation de l'orchestrateur de domaine

L'orchestrateur de domaine est installé lorsque vous installez CA Process Automation pour la première fois. Certaines conditions doivent être remplies préalablement à son installation. Vous pouvez utiliser un assistant d'installation pour installer l'orchestrateur de domaine de façon interactive. Ou, vous pouvez créer un fichier de réponse sans attribuer de valeurs par défaut aux paramètres, puis exécuter le script pour installer l'orchestrateur de domaine de façon silencieuse. Une fois l'installation terminée, configurez les ports et le pare-feu, puis configurez CA Process Automation en procédant comme décrit dans le *Manuel de l'administrateur de contenu*.

Ce chapitre traite des sujets suivants :

Conditions préalables à l'installation de l'orchestrateur de domaine (page 65)
Installation interactive de l'orchestrateur de domaine (page 93)
Installation autonome de l'orchestrateur de domaine (page 118)
Tâches de post-installation liées à l'orchestrateur de domaine (page 125)
Désinstallation de l'orchestrateur de domaine (page 140)

Conditions préalables à l'installation de l'orchestrateur de domaine

Envisagez la possibilité de configurer un équilibreur de charge lors de la première installation en vue de son extension future. Vous pouvez ajouter des noeuds de cluster lorsque que cela s'avère nécessaire.

Remarque : Il est recommandé d'utiliser un équilibreur de charge matérielle. Voir Conditions requises pour l'équilibreur de charge F5 (page 53) Si cela n'est pas possible, il est recommandé de choisir NGINX comme équilibreur de charge logicielle. NGINX pour UNIX s'adapte très facilement. NGINX pour Windows peut prendre en charge jusqu'à 300 agents à l'aide de la communication simplifiée. Voir Conditions requises pour l'équilibreur de charge NGINX

Planifiez l'installation initiale de CA Process Automation. Pour les conditions requises des composants, reportez-vous à la section suivante :

- Prise en charge des plates-formes et conditions requises pour les composants CA Process Automation (page 30)
- Configuration matérielle requise (page 32)

Procédez comme suit :

1. Identifiez un hôte pour l'orchestrateur de domaine qui satisfait la configuration requise.
2. Vérifiez que l'hôte de l'orchestrateur de domaine dispose d'un kit de développement Java pris en charge.

   Voir Configuration requise pour le kit de développement Java (page 77)
3. Le cas échéant, activez la localisation des composants pris en charge sur l'hôte équipé de l'orchestrateur de domaine.

   Voir Détermination de l'emplacement des composants pris en charge (page 67)
4. Identifiez le serveur de base de données sur lequel les bases de données de la bibliothèque, de reporting et d'exécution de l'orchestrateur de domaine doivent être installées.
5. Préparez le serveur de base de données.

   Voir Conditions requises pour le serveur de base de données (page 69)
6. Identifiez l'hôte de CA EEM, si un produit CA EEM n'est pas déjà utilisé avec un autre produit CA Technologies.
7. Déterminez les options de configuration de CA EEM.

   Voir Conditions requises pour CA EEM (page 79), notamment Conditions préalables à la configuration de l'authentification NTLM.
8. Si CA EEM est configuré avec CA SiteMinder, prévoyez de configurer CA Process Automation de sorte à utiliser la fonctionnalité d'authentification unique.

   Voir Utilisation de CA SiteMinder avec CA Process Automation (page 219)
9. Vous pouvez configurer un équilibreur de charge si vous prévoyez la mise en cluster nécessaire de l'orchestrateur de domaine ultérieurement. Consultez la section Configuration d'un équilibreur de charge pour la mise en cluster de l'orchestrateur (page 35).
10. Enregistrez dans un endroit sécurisé le mot de passe de certificat que vous voulez définir dans le champ Mot de passe du certificat de l'orchestrateur de domaine.

    Important : Vous devez fournir le même mot de passe lorsque vous installez d'autres orchestrateurs ou des noeuds d'orchestrateur supplémentaires. Si vous oubliez le mot de passe, vous devez réinstaller tous les orchestrateurs dans votre système en commençant par l'orchestrateur de domaine. Ce même mot de passe est requis lors de la mise à niveau vers une nouvelle version.

Détermination de l'emplacement des composants pris en charge

La définition d'un système CA Process Automation consiste en partie à déterminer les nouveaux composants que vous pouvez installer sur le même hôte de l'orchestrateur de domaine CA Process Automation et ceux que vous pouvez installer sur des serveurs distincts. Prenons les composants de réseau CA Process Automation ci-dessous.

- Kit de développement Java : doit être installé.
- CA Embedded Entitlements Manager (CA EEM) : peut être installé, mais ce n'est pas recommandé.
- Serveurs de base de données CA Process Automation : peut être installé, mais ce n'est pas recommandé.
- Equilibreur de charge (pour la mise en cluster) : ne peut pas être installé.
- Autres orchestrateurs : ne peut pas être installé.
- Noeuds de cluster : ne peuvent pas être installés.
- Serveur NTP : externe au réseau
- CA SiteMinder (facultatif) : peut être installé, mais cela est déconseillé.

Tous les noeuds de cluster et orchestrateurs sont généralement installés sur un hôte distinct. Le serveur NTP peut être externe au réseau.

Pour une version légère de CA Process Automation, vous pouvez installer les entités suivantes sur l'hôte sur lequel vous avez installé l'orchestrateur de domaine :

- CA EEM
- Serveur pour les bases de données de bibliothèque, de reporting et d'exécution.

Prenez en compte les facteurs ci-dessous lors de l'évaluation de l'option idéale : installation d'entités ou utilisation de plusieurs hôtes.

- Caractéristiques de l'hôte

  Il s'agit principalement de la quantité et de la vitesse des unités centrales, de la mémoire, des espaces de stockage sur disque et des réseaux.

- Volume de processus

  Vous devez prendre en compte le nombre total de processus, ainsi que leurs taux soutenus maximum pendant des périodes de pic de l'activité.

- Implémentation des processus

  Tous les processus ne sont pas identiques : certains utilisent peu d'opérateurs, d'autres en utilisent des centaines. Certains processus incluent un grand nombre d'activités requérant une quantité élevée d'UC, tandis que d'autres consacrent la plupart de leur temps à attendre que des événements ou des interactions utilisateur aient lieu. Ceci rend difficile la spécification de la charge en termes de volume/taux de processus. Le débit varie y compris avec la granularité d'opérateurs la plus fine.

- Niveau requis de réactivité

  La réactivité en temps réel n'est jamais accessible avec l'implémentation actuelle. Toutefois, des exigences moins rigoureuses entrent en compte lorsque d'autre matériel est nécessaire pour les orchestrateurs supplémentaires. Lorsque l'accord sur les niveaux de service (SLA) est restrictif, le système a besoin de davantage de capacité de réserve pour qu'aucun ralentissement ne soit noté pendant les périodes de pointe. Sans SLA, le système a besoin uniquement de la capacité suffisante pour couvrir la charge moyenne.

- Intensité d'utilisation pour les composants partagés

  Prenez en compte les autres utilisations faites de CA EEM et du système SGBDR.

En prévision de la croissance future, nous recommandons de ne pas installer CA EEM et le serveur de base de données sur le même serveur que l'orchestrateur de domaine. La seule façon sûre de déterminer les circonstances dans lesquelles les ressources sont suffisantes consiste à tester la charge complète.

Conditions requises pour le serveur de base de données

CA Process Automation requiert un ou plusieurs des serveurs de base de données tiers suivants pour stocker et conserver ses données :

- MySQL Server 5.5
- Microsoft SQL Server 2005, 2008, 2008 R2, 2012
- Base de données Oracle 10g version 2 ou 11g version 2

CA Process Automation contient trois bases de données. Chacune de ces bases de données peut résider dans le même serveur de base de données, dans différents serveurs de base de données du même type, ou dans des serveurs de base de données de types différents.

Si vous ne disposez pas déjà de l'un de ces serveurs, consultez les conditions requises pour chacun d'eux avant d'en faire l'acquisition. Il est recommandé d'installer ce serveur et CA Process Automation sur des hôtes distincts.

Suivez les directives relatives au type de serveur de base de données que vous utilisez pour l'installation de l'orchestrateur.

- Préparation d'un serveur MySQL Server pour CA Process Automation (page 72)
- Préparation d'un serveur Microsoft SQL Server pour CA Process Automation (page 73)
- Préparation du serveur de base de données Oracle pour CA Process Automation (page 75).

A propos des bases de données CA Process Automation

Chaque orchestrateur requiert trois bases de données logiques :

- La base de données de référentiel, également appelée *base de données de bibliothèque*, est la base de données dans laquelle sont stockés les objets d'automatisation créés dans les dossiers de l'onglet Bibliothèque de CA Process Automation. Les données stockées incluent l'arborescence de bibliothèque, la définition complète de chaque objet, ainsi que les informations concernant la propriété et le contrôle de version.

  Remarque : Plusieurs orchestrateurs peuvent utiliser la base de données de référentiel de l'orchestrateur de domaine ou chaque orchestrateur peut posséder la sienne.

- La *base de données d'exécution* est une base de données spécifique de l'orchestrateur dans laquelle sont stockées les données des instances de processus d'un orchestrateur unique ou d'un cluster d'orchestrateur. Il peut s'agir d'informations concernant les instances de processus en cours d'exécution, les instances qui ont été exécutées, mais qui n'ont pas encore été déplacées vers la table d'archivage ou les instances archivées. Vous pouvez accéder aux données actuelles et archivées à partir de l'onglet Opérations. Chaque enregistrement d'exécution inclut l'état, l'ensemble de données et le propriétaire de l'instance d'objet ainsi que les informations de planification.

  Remarque : Chaque orchestrateur requiert une base de données d'exécution distincte. Un orchestrateur autonome dispose de sa propre base de données. Un cluster d'orchestrateur est considéré comme un orchestrateur logique unique ; dans ce cas, tous les noeuds partagent la même base de données.

- La *base de données de reporting* stocke des données historiques des instances de processus et d'opérateur. Les administrateurs peuvent utiliser ces données pour générer des rapports à une vitesse proche du temps réel grâce aux définitions de rapport prédéfinies et aux définitions de rapport personnalisées disponibles dans l'onglet Rapports.

  Remarque : La base de données de reporting est généralement partagée entre tous les orchestrateurs.

Ces bases de données logiques peuvent partager une base de données physique, mais il est conseillé d'utiliser des bases de données distinctes. Les noms des bases de données de CA Process Automation ne doivent pas respecter la casse.

Il est recommandé de réserver un espace disque minimum de 40 Go pour vos bases de données. Certaines opérations, telles que la mise à niveau de CA Process Automation, peuvent requérir une quantité élevée de ressources. Nous vous recommandons d'utiliser suffisamment d'espace et de surveiller régulièrement l'espace consommé.

Remarques sur la politique d'archivage

- Les bases de données d'exécution augmentent à mesure que les processus sont exécutés et l'espace requis pour le stockage de ces données dépend de la taille du contenu des instances de processus ainsi que des paramètres de la politique d'archivage de CA Process Automation.
- Les instances de processus sont stockées en fonction de la politique d'archivage. Vous pouvez configurer la politique de purge d'archives pour réaliser les actions suivantes :
  - Déplacer des instances vers l'archivage après une certaine période de temps
  - Supprimer automatiquement des instances anciennes sans les déplacer vers l'archivage
  - Aucune action

    Remarque : Lorsque la politique est définie pour ne réaliser aucune action, il est recommandé d'effectuer des tâches d'archivage de données en dehors de CA Process Automation.
- La politique d'archivage est spécifique à l'orchestrateur.

Remarque : Consultez la section Configuration des politiques d'orchestrateur dans le *Manuel de l'administrateur de contenus*.

Informations complémentaires :

Options de configuration avancée (page 20)

Préparation d'un serveur MySQL Server pour CA Process Automation

Lors de l'installation de l'orchestrateur de domaine ou d'un orchestrateur supplémentaire, le programme d'installation crée des bases de données CA Process Automation au niveau du serveur MySQL spécifié. Le programme d'installation requiert les éléments suivants :

- Pendant l'installation, accédez au pilote JDBC MySQL. Ce pilote n'est pas inclus dans le média d'installation CA Process Automation.

  Remarque : Il est recommandé d'utiliser le pilote JDBC MySQL version 5.1.7 et ultérieure.
- Informations d'identification de l'utilisateur avec des droits d'administration pour créer les bases de données de la bibliothèque, de reporting et d'exécution.
- Deux variables MySQL personnalisées pour CA Process Automation.

Avant d'installer un orchestrateur qui utilise le serveur de base de données MySQL, préparez le serveur MySQL pour CA Process Automation.

Procédez comme suit :

1. Téléchargez le pilote JDBC à partir du site Web MySQL, MySQL Connector/J 5.1.7 par exemple.
2. Enregistrez le pilote à un emplacement auquel vous pouvez accéder pendant l'installation.
3. Ouvrez MySQL Workbench et sélectionnez le fichier d'options (Options File) sous Configuration.
4. Définissez la durée d'attente du verrouillage des transactions avant leur rétablissement :
   a. Sélectionnez l'onglet InnoDB.
   b. Accédez au groupe Various.
   c. Sélectionnez innodb_lock_wait_timeout.
   d. Remplacez la valeur par défaut (50) par une valeur supérieure à 60.

      ```
      innodb_lock_wait_timeout = 90
      ```

5. Définissez la longueur de paquet maximum sur 33554432 octets (32 Mo) pour l'envoi vers le serveur et la réception à partir de celui-ci. La valeur par défaut est 1048576.
   a. Cliquez sur l'onglet Networking.
   b. Localisez le groupe Data/Memory size.
   c. Sélectionnez max_allowed_packet.
   d. Entrez la valeur requise.
6. Cliquez sur Appliquer.

   Un message de confirmation des changements à appliquer au fichier de configuration MySQL s'affiche.

Préparation de Microsoft SQL Server pour CA Process Automation

Avant d'installer l'orchestrateur de domaine CA Process Automation (ou un orchestrateur supplémentaire) sur lequel les bases de données CA Process Automation résident au niveau du serveur SQL Server, procédez comme suit :

- Vérifiez que le serveur SQL Server présente la configuration requise pour CA P (page 74)rocess Automation.
- Etudiez le mode de référencement du pilote JDBC 3.0 (page 74).
- Vérifiez les directives permettant de spécifier le nom de serveur de base de données pour SQL Server (page 75).

Vérification de la configuration requise par CA Process Automation au niveau du serveur SQL Server

Le serveur SQL Server que vous préparez pour les bases de données CA Process Automation doit présenter la configuration requise suivante :

- Le serveur SQL Server doit être installé ou configuré avec l'authentification en mode mixte. Vous devez spécifier un compte avec l'authentification SQL Server lors de l'installation de l'orchestrateur.
- Le programme d'installation de l'orchestrateur requiert des informations d'identification de l'utilisateur possédant des droits d'administration pour créer les bases de données CA Process Automation.
- Le classement SQL Server des bases de données CA Process Automation doit être SQL_Latin1_General_CP1_CI_AS. Par défaut, le programme d'installation CA Process Automation utilise ce classement pour créer des bases de données.

Pour vérifier que votre serveur SQL Server rempli les conditions requises par CA Process Automation, consultez le fichier de configuration de votre serveur SQL Server.

Procédez comme suit :

1. Accédez au fichier ConfigurationFile.ini dans un chemin d'accès semblable à celui ci-dessous :

   ```
   C:\ Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\ yyyymmdd_hhmmss
   ```

2. Vérifiez que le paramètre de mode de sécurité ressemble à celui ci-dessous :

   ```
   ; La valeur par défaut est l'authentification Windows. Utilisez « SQL » pour l'authentification en mode mixte.

   SECURITYMODE="SQL"
   ```

3. Vérifiez que le paramètre pour les informations d'identification de compte d'administrateur système SQL est semblable à celui ci-dessous :

   ```
   ; Compte(s) Windows à configurer avec des privilèges d'accès d'administrateur système SQL Server.
   SQLSYSADMINACCOUNTS=".\Administrator"
   ```

4. Vérifiez que le paramètre pour le classement est semblable à celui ci-dessous :

   ```
   ; Spécifie un classement Windows ou SQL à utiliser pour le moteur de base de données.
   SQLCOLLATION="SQL_Latin1_General_CP1_CI_AS"
   ```

Mode de référencement du pilote JTDS JDBC

Lors de l'installation de l'orchestrateur, le pilote JTDS 1.3 pour SQL Server (inclus dans le dossier DVD1) est requis par le programme d'installation. Chemin d'accès :

```
.../DVD1/drivers/jtds-1.3.jar
```

Directives pour la spécification du nom de serveur de base de données pour SQL Server

Lorsque vous installez l'orchestrateur de domaine ou un orchestrateur non mis en cluster, vous entrez des informations pour trois bases de données CA Process Automation : Bibliothèque, Exécution et Reporting. Si vous définissez le type de base de données MS SQL, appliquez les directives suivantes pour spécifier le serveur de base de données :

- Si vous disposez uniquement d'une instance SQL Server sur le serveur hôte, spécifiez le nom d'hôte du serveur. Ce nom est l'instance par défaut.
- Si vous disposez de plusieurs instances SQL Server sur le serveur hôte, spécifiez l'instance nommée SQL Server au format *nom_hôte**instance_nommée*.

  Une instance nommée SQL Server est une copie de SQL Server exécutée sur le même hôte. Chaque copie est exécutée indépendamment et distinguée par son nom d'instance. Un serveur de base de données peut contenir plusieurs instances nommées, mais uniquement une instance par défaut (non nommée).

Préparation du serveur de base de données Oracle pour CA Process Automation

Les opérations de préparation suivantes sont requises avant d'installer l'orchestrateur de domaine ou un orchestrateur supplémentaire qui utilise Oracle pour héberger ses bases de données internes.

Procédez comme suit :

1. Créer un utilisateur avec des droits de connexion et d'accès aux ressources.
2. Vérifiez que l'espace disque logique au niveau d'Oracle est suffisant pour l'hébergement des bases de données suivantes :
   - Base de données de bibliothèque
   - base de données d'exécution
   - base de données de reporting

3. Créez les bases de données de bibliothèque, de reporting et d'exécution manuellement.
4. Configurez les paramètres suivants :
   - Définissez les connexions sur 100 au maximum (ou sur 150 au minimum pour les clusters).

     Toutes les connexions sont effectuées via les orchestrateurs, mais certaines connexions unies sont requises pour un comportement optimal.
   - Activez le traitement de transaction en ligne (Online transaction Processing, OLTP) pour faciliter les transactions
5. Etudiez le mode de référencement du pilote JDBC pour Oracle.

   Le pilote JDBC pour Oracle (inclus dans le dossier DVD1) est requis par le programme d'installation pendant l'installation de l'orchestrateur. Chemin d'accès :

   ```
   .../DVD1/drivers/ojdbc14.jar
   ```

Remarques :

- Le partitionnement n'est *pas* pris en charge.

Droits de propriétaire de base de données

Lorsque vous démarrez CA Process Automation pour la première fois ou que vous appliquez un correctif, l'application adapte la structure de la base de données ou du schéma.

Les droits de base de données minimum requis par CA Process Automation sont les suivants :

- Droit d'accès aux métadonnées (pour déterminer la structure)
- Droit de créer/modifier/supprimer des droits DDL (langage de définition de données) pour des tables, des index, des vues, des contraintes et des séquences inclus dans la base de données
- Droits de lecture ou d'écriture sur toutes les tables

Les tables de l'application CA Process Automation requièrent les droits suivants :

- Sélectionner
- Insérer
- Supprimer

Configuration requise pour le kit de développement Java

Avant d'installer un orchestrateur, vérifiez que la configuration requise du kit de développement Java est respectée. Exécutez la commande suivante :

```
Java –version
```

```
C:\>Java -version
java version "1.7.0_45"
Java(TM) SE Runtime Environment (build 1.7.0_45-b18)
Java HotSpot(TM) 64-Bit Server VM (build 24.45-b08, mixed mode)
```

L'exemple précédent illustre une version Java valide pour Windows.

Procédez comme suit :

1. Connectez-vous à l'hôte sur lequel vous voulez installer l'orchestrateur de domaine.
2. Vérifiez que vous disposez du kit de développement Java 1.7 d'Oracle.

   Remarque : Pour plus d'informations, consultez la section Prise en charge des plates-formes et conditions requises pour les composants CA Process Automation (page 30). Si la version Java par défaut est différente, modifiez-la sur le shell sur lequel vous allez démarrer le programme d'installation de CA Process Automation.
3. Si la version du JDK requis n'est pas installée, téléchargez-la à partir du site Web Oracle et exécutez l'assistant d'installation pour installer le kit de développement Java.
4. Dans le cas d'un orchestrateur mis en cluster, vérifiez que le kit de développement Java d'Oracle est installé sur chaque noeud.

Définition du chemin d'accès au répertoire de base Java par défaut

Si la version par défaut est différente, modifiez la version Java par défaut sur le shell sur lequel vous allez démarrer l'installation de CA Process Automation.

Procédez comme suit :

1. Accédez au dossier DVD1.
2. Définissez la version Java par défaut sur l'invite de commande ou le shell.

   Windows

   ```
   définissez JAVA_HOME=<home_directory_of_jdk (not_bin)>
   définissez PATH=%JAVA_HOME%\bin;%PATH%
   ```

   UNIX ou Linux

   ```
   exportez JAVA_HOME=<home_directory_of_jdk (not_bin)>
   exportez PATH=$JAVA_HOME/bin:$PATH
   ```

3. Démarrez le programme d'installation à partir de cette invite de commande ou ce shell.

   Windows

   ```
   .\ Domain_Installer_windows.bat
   ```

   UNIX ou Linux

   ```
   ./ Domain_Installer_unix.sh
   ```

   Le programme d'installation lance d'abord le programme d'installation tiers, puis le programme d'installation de l'orchestrateur de domaine.

Conditions préalables pour CA EEM

CA Process Automation utilise CA Embedded Entitlements Manager (CA EEM) pour l'authentification et l'autorisation des utilisateurs. Le produit CA EEM est requis.

- Si vous utilisez CA EEM avec un autre produit CA Technologies, vérifiez si la version est prise en charge par CA Process Automation. Consultez la section Prise en charge des plates-formes et conditions requises pour des composants CA Process Automation (page 30).
- Si vous n'avez pas installé CA EEM ou si votre version de CA EEM est antérieure aux versions prises en charge par CA Process Automation, téléchargez et installez CA EEM (page 80).
- Déterminez la méthode d'authentification des utilisateurs de CA Process Automation (page 86).
- Collectez les informations relatives à CA EEM nécessaires à l'installation de l'orchestrateur de domaine (page 82).
- Pour créer deux instances CA EEM lors de l'installation, l'une pour l'utilisation et l'autre en cas de basculement, reportez-vous à la section Préparation du basculement vers un serveur CA EEM de secours (page 81). Cette procédure est facultative et peut être effectuée ultérieurement.

Configuration de CA EEM

CA Process Automation requiert CA EEM pour gérer les autorisations et les authentifications. Avant l'installation ou la mise à niveau de CA Process Automation, une instance de CA EEM appropriée doit être disponible. CA Process Automation peut utiliser une version de CA EEM de 8.4 SP04 CR10 à 12.5.1, mais certaines de ses fonctionnalités ne sont plus prises en charge dans toutes les versions de CA EEM. Exemple :

La prise en charge des certificats de sécurité 2048 et 4096 bits requiert la version 12.0 de CA EEM ou une version ultérieure.

La prise en charge de plusieurs domaines Microsoft Active Directory requiert CA EEM 12.5 ou une version ultérieure.

Si votre site dispose d'une instance de CA EEM existante qui n'est pas la version requise, consultez l'administrateur de votre site pour vérifier que l'instance de CA EEM peut être mise à niveau vers la version de votre choix. Les restrictions de prise en charge de version d'autres produits à l'aide de l'instance de CA EEM peuvent empêcher la mise à niveau de l'instance.

Nouvelle installation de CA EEM

Une nouvelle installation de CA EEM est requise si aucune instance de CA EEM dans la version de votre choix n'est disponible.

Procédez comme suit :

Téléchargez des programmes d'installation pour CA EEM 12.5.1 à partir de l'emplacement du média d'installation de CA Process Automation.

Lors du déploiement ou de la mise à niveau de l'instance de CA EEM, suivez les instructions fournies dans la documentation de CA EEM.

Remarques sur la configuration de CA EEM

Lorsque vous configurez CA EEM de sorte à utiliser le référentiel d'utilisateurs interne ou un référentiel d'utilisateurs externe, tenez compte des conséquences suivantes pour CA Process Automation :

Si vous sélectionnez le référentiel d'utilisateurs par défaut, créez des comptes pour les utilisateurs CA Process Automation. Les informations d'identification de l'utilisateur définies dans CA EEM sont utilisées pour l'authentification lors de la connexion.

Si vous indiquez un référentiel d'utilisateurs externe, les comptes d'utilisateurs de ce référentiel sont automatiquement chargés dans CA EEM comme utilisateurs globaux. Les informations d'identification de l'utilisateur définies dans l'annuaire Microsoft Active Directory référencé sont utilisées pour l'authentification.

Reportez-vous à la section Référencement d'utilisateurs globaux et de groupes globaux à partir de Microsoft Active Directory (page 91). (CA EEM 8.4)

Consultez la rubrique Référencement d'utilisateurs globaux à partir de plusieurs annuaires Active Directory (page 91). (CA EEM 12.51)

Lorsque vous configurez CA EEM en mode FIPS, tenez compte de ce qui suit :

CA Process Automation chiffre les données transférées entre CA Process Automation et CA EEM.

Si vous sélectionnez le mode FIPS dans CA EEM, CA Process Automation doit être configuré de manière à utiliser les algorithmes pris en charge par FIPS pour les communications entre CA Process Automation et CA EEM. Pendant l'installation de CA Process Automation, sélectionnez Utiliser le certificat conforme à la norme FIPS pour utiliser des algorithmes pris en charge par FIPS.

Préparation du basculement vers un serveur CA EEM de secours

Dans une configuration de haute disponibilité, il est recommandé de configurer deux instances CA EEM. De cette façon, le serveur CA EEM principal sert de serveur d'authentification et d'autorisation de sécurité actif pour CA Process Automation. Le serveur CA EEM secondaire est le serveur d'authentification et d'autorisation de sécurité de secours. Ce dernier met en miroir le serveur CA EEM principal. Les deux instances de CA EEM peuvent pointer vers le même répertoire externe.

De manière automatique et transparente, CA Process Automation bascule du serveur CA EEM principal vers le serveur CA EEM secondaire en cas d'échec du premier suite à la connexion initiale de CA Process Automation. Le basculement se produit même si le serveur principal est arrêté lorsque vous configurez les deux serveurs CA EEM dans CA Process Automation.

Pour obtenir des informations sur la configuration de CA EEM dans une configuration de haute disponibilité, consultez la documentation CA EEM correspondant à la version déployée sur votre site. Des informations complémentaires sont disponibles à la page Meilleures pratiques d'implémentation de CA Process Automation, accessible via un lien rapide dans l'onglet Accueil de CA Process Automation.

Collecte des informations relatives à CA EEM nécessaires à l'installation de l'orchestrateur de domaine

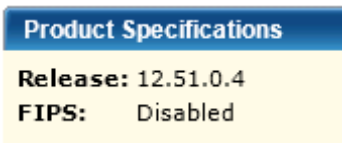
Avant de démarrer l'installation de l'orchestrateur de domaine, rassemblez les informations suivantes sur la configuration de CA EEM :

- Les informations d'identification de l'administrateur CA EEM, où EiamAdmin est le nom d'utilisateur.
- La version de compilation de CA EEM et le paramètre FIPS dans CA EEM.

  1. Accédez au serveur CA EEM que vous utilisez.

     `https://serveur:5250/spin/eiam`

  2. Sélectionnez le nom de l'application CA Process Automation dans la liste déroulante Application.
  3. Entrez des informations d'identification valides, **EiamAdmin** et le mot de passe associé. Cliquez sur Connexion.
  4. Cliquez sur A propos de. La version de compilation de CA EEM et le paramètre FIPS s'affichent sous Caractéristiques du produit.



Remarque : Pendant l'installation de CA Process Automation, le processus qui enregistre l'application CA Process Automation dans CA EEM génère également les certificats que CA Process Automation utilise pour se connecter à CA EEM.

- Si le mode FIPS est activé dans CA EEM, PAM.cer et PAM.key sont générés.
- Si le mode FIPS est désactivé dans CA EEM, fournissez un mot de passe (le mot de passe du certificat CA EEM) avant d'enregistrer l'application CA Process Automation dans CA EEM. Ce mot de passe est utilisé pour protéger le certificat PAM.p12 généré après l'enregistrement de l'application CA Process Automation dans CA EEM.
- Si vous installez l'application CA Process Automation *sans l'enregistrer* dans CA EEM, vous êtes invité à sélectionner le kit de développement logiciel correspondant à la version du serveur CA EEM.

- Nom d'hôte du serveur CA EEM. Pour déterminer le nom d'hôte, connectez-vous à CA EEM. Le nom d'hôte est affiché avec l'étiquette Arrière-plan dans la barre de titre.

  Important : Vous avez besoin du mot de passe EiamAdmin pour vous connecter à CA EEM.

- Si vous procédez à la mise à niveau et prévoyez de configurer CA EEM de façon à utiliser plusieurs annuaires Microsoft Active Directory, notez le nom du domaine Active Directory que vous référencez. Spécifiez ce domaine en tant que domaine Active Directory par défaut. Les utilisateurs de CA Process Automation appartenant au domaine Active Directory par défaut peuvent se connecter à CA Process Automation avec leur nom d'utilisateur non qualifié après leur réaffectation à un groupe d'applications.
- Enregistrez le mot de passe de certificat que vous prévoyez de saisir. Ce mot de passe de certificat contrôle l'accès aux clés utilisées pour chiffrer des mots de passe et d'autres données critiques. Le mot de passe du certificat est propre à un domaine CA Process Automation unique. Ce mot de passe de certificat n'est pas lié à CA EEM, mais il est important de l'enregistrer.

  Important : Utilisez ce mot de passe lorsque vous installez un autre orchestrateur ou que vous ajoutez des noeuds de cluster à un orchestrateur. Ce même mot de passe est une entrée requise lors de la mise à niveau de CA Process Automation.

Identification de la version du kit de développement logiciel CA EEM utilisé par CA Process Automation

Vous pouvez déterminer si la version du kit de développement logiciel de CA EEM utilisé par CA Process Automation est la version 8 ou 12.

Procédez comme suit :

1. Arrêtez l'orchestrateur de domaine.
2. Augmentez le niveau de journalisation de l'orchestrateur de domaine sur INFO.
3. Lancez l'orchestrateur de domaine.
4. Connectez-vous au serveur CA Process Automation.
5. Révisez les journaux.
   - Si CA Process Automation utilise le kit de développement logiciel CA EEM r8.4 :

     ```
     13:03:16,859 INFO
     [com.optinuity.c2o.eemconfiguration.EEMManagerFactory]
     (http-user01-m4600.ca.com-138.42.24.149-8080-2) Found
     method: soRetrieveByUserName in class:
     com.ca.eiam.SafeGlobalUser. La version actuelle du kit de
     développement logiciel EEM est 8.
     13:03:16,861 INFO
     [com.optinuity.c2o.eemconfiguration.EEM8Manager]
     (http-user01-m4600.ca.com-138.42.24.149-8080-2) Initialized
     EEM8Manager...
     ```

   - Si CA Process Automation utilise le kit de développement logiciel CA EEM 12.51 :

     ```
     13:32:37,195 INFO
     [com.optinuity.c2o.eemconfiguration.EEMManagerFactory]
     (http-user02-M4600.ca.com-138.42.24.149-8080-2) Found
     method: soRetrieveByPrincipalName in class:
     com.ca.eiam.SafeGlobalUser. La version actuelle du kit de
     développement logiciel EEM est 12.
     13:32:37,198 INFO
     [com.optinuity.c2o.eemconfiguration.EEM12Manager]
     (http-user02-M4600.ca.com-138.42.24.149-8080-2) Initialized
     EEM12Manager...
     ```

6. Arrêtez l'orchestrateur de domaine, redéfinissez le niveau de journalisation sur le niveau précédent, puis redémarrez l'orchestrateur de domaine.

Conditions préalables à la configuration de l'authentification NTLM

Avant de configurer l'authentification NTLM, effectuez les opérations suivantes :

- Vérifiez que CA EEM est installé sur un serveur avec un système d'exploitation Microsoft Windows.
- Vérifiez que CA EEM utilise Microsoft Active Directory comme référentiel d'utilisateurs externe.
- Vérifiez que CA EEM n'est pas configuré pour plusieurs domaines Active Directory ou pour une forêt Active Directory.
- Vérifiez que les utilisateurs accèdent à CA Process Automation à partir d'un ordinateur Windows.
- Vérifiez que le serveur CA EEM et l'ordinateur à partir duquel les utilisateurs accèdent à CA Process Automation sont présents dans le même domaine de réseau. Si les ordinateurs font partie de domaines imbriqués, veillez à ce que le serveur CA EEM et l'ordinateur à partir duquel l'application est lancée appartiennent à des domaines disposant d'une relation de confiance.
- Vérifiez que les utilisateurs du domaine sont ajoutés aux groupes d'utilisateurs sur l'ordinateur à partir duquel l'application est lancée.

Méthode d'authentification des utilisateurs de CA Process Automation à utiliser

Si vous procédez à une nouvelle installation de CA Process Automation, une partie de la préparation consiste à déterminer la méthode d'authentification des utilisateurs CA Process Automation. La configuration décrite ici est effectuée une fois que l'installation est terminée. Toutefois, les options d'installation de CA Process Automation que vous sélectionnez dépendent de votre planification. Les options incluent :

- Créez un compte d'utilisateur pour chaque utilisateur CA Process Automation dans CA EEM. L'administrateur de CA EEM affecte un ID d'utilisateur à chaque compte. Les utilisateurs peuvent changer leur propre mot de passe dans CA EEM. Lorsque les utilisateurs se connectent à CA Process Automation, CA EEM les authentifie en vérifiant que l'ID d'utilisateur et le mot de passe saisis (informations d'identification) appartiennent à un compte d'utilisateur actif.
- Référencement des comptes d'utilisateurs stockés dans un ou plusieurs domaines Microsoft Active Directory. CA EEM transmet les informations d'identification utilisées pour la connexion de CA Process Automation à Active Directory ; Active Directory effectue l'authentification.
- Utilisez l'authentification directe NTLM sans CA SiteMinder. Le référencement des comptes d'utilisateurs stockés dans un domaine Microsoft Active Directory est requis. L'authentification NTLM n'est pas prise en charge si vous référencez plusieurs domaines Microsoft Active Directory. L'authentification NTLM requiert que tous les ordinateurs affectés utilisent un système d'exploitation Windows et soient présents dans le même domaine ou dans des domaines dont les relations sont approuvées.
- Activez l'authentification unique à l'aide de l'authentification NTLM. Pour ce faire, utilisez CA SiteMinder ou appliquez les conditions préalables à la configuration de l'authentification NTLM. (page 85) Dans les deux cas, sélectionnez l'authentification NTLM lors de l'installation. NTLM gère l'authentification lorsque les utilisateurs accèdent à CA Process Automation. Les utilisateurs authentifiés sont connectés à l'aide de leurs informations d'identification Windows. Vous pouvez également activez l'authentification directe NTLM après l'installation (page 131).

S'il s'agit d'une nouvelle installation CA Process Automation, une partie de la préparation détermine la procédure d'authentification des utilisateurs CA Process Automation. La configuration proprement dite décrite ici est effectuée à l'issue de l'installation. Toutefois, la méthode d'authentification sélectionnée détermine les paramètres spécifiés lors de l'installation de CA Process Automation. Les options d'authentification sont les suivantes :

Authentification EEM-based

- Utilisateur EEM natif

  Configuration requise

  - Installation de CA EEM

Détails : un administrateur de CA EEM crée un compte dans CA EEM pour chaque utilisateur devant accéder à CA Process Automation. L'administrateur de CA EEM fournit à chaque utilisateur un ID de connexion. Les utilisateurs peuvent changer leur propre mot de passe dans CA EEM. Lorsque les utilisateurs se connectent à CA Process Automation, CA EEM les authentifie en vérifiant que l'ID d'utilisateur et le mot de passe saisis (informations d'identification) appartiennent à un compte d'utilisateur actif.

Action requise lors de l'installation de CA Process Automation

Aucune action spécifique n'est requise.

Référence à l'annuaire LDAP

Configuration requise

Installation de CA EEM

Accès à un annuaire LDAP externe

Détails : les types et configurations d'annuaire suivants sont disponibles :

Active Directory

Vous pouvez configurer CA EEM de sorte à référencer les comptes d'utilisateurs stockés dans un ou plusieurs annuaires Microsoft Active Directory. CA Process Automation transmet à CA EEM les informations d'identification et CA EEM les transfère à Active Directory pour leur validation.

Annuaire LDAP autre qu'Active Directory

Vous pouvez également configurer CA EEM pour utiliser un annuaire LDAP autre qu'Active Directory. L'authentification est gérée de la même manière dans ce cas.

Action requise lors de l'installation de CA Process Automation

Aucune action spécifique n'est requise.

Authentification unique à l'aide de l'authentification NTLM

Configuration requise

Les mêmes conditions préalables requises que celles décrites plus haut pour l'utilisation d'Active Directory avec l'option d'annuaire LDAP s'appliquent.

(NEED TO VERIFY if NTLM authentication is not supported if you reference multiple Microsoft AD domains.)

De plus, vous devez respecter les conditions requises pour configurer l'authentification NTLM.

Remarque : L'une des conditions requises repose sur l'utilisation d'un système d'exploitation Windows par les utilisateurs PAM et sur leur présence dans le même domaine que celui du serveur EEM, ou dans des domaines dont les relations sont approuvées.

Détails : CA EEM gère l'authentification via NTLM lorsque les utilisateurs accèdent à CA Process Automation. Les utilisateurs authentifiés sont connectés à l'aide de leurs informations d'identification Windows.

Action requise lors de l'installation de CA Process Automation

Lors de l'installation de CA Process Automation, sélectionnez [Option NTLM] dans la page de l'assistant CA EEM. Cette méthode est recommandée pour activer l'authentification unique.

Remarque : Vous pouvez activer l'authentification directe NTLM à l'issue de l'installation, le cas échéant.

Authentification SiteMinder-based

Authentification unique à l'aide de CA SiteMinder

Configuration requise

[Point to SiteMinder doc]

Détails : CA SiteMinder effectue l'authentification à l'aide d'un annuaire externe et envoie le nom d'utilisateur à CA Process Automation. L'utilisateur est alors autorisé à accéder à CA EEM. [We should probably point the user to the SiteMinder section in our install guide for more details.]

Action requise lors de l'installation de CA Process Automation

Le nom d'hôte et les en-têtes SiteMinder sont spécifiés dans la page de l'assistant d'équilibrage de la charge.

Authentification et autorisation d'utilisateur en mode FIPS

Vous pouvez configurer CA EEM pour utiliser le mode FIPS. Cette option est disponible. CA Process Automation peut uniquement être configuré pour utiliser le mode FIPS si CA EEM est également configuré pour utiliser ce mode. Toutefois, CA Process Automation peut être configuré pour ne pas utiliser le mode FIPS, même si CA EEM est configuré pour l'utiliser.

Que le mode FIPS soit défini sur Activé ou Désactivé, les données transférées entre CA EEM et CA Process Automation seront chiffrées. Les algorithmes utilisés pour le chiffrement sont différents.

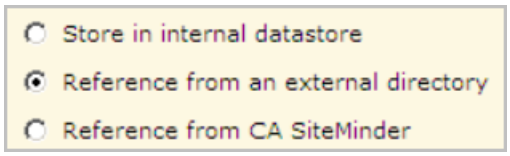
Lorsque les utilisateurs se connectent, CA Process Automation transfère le nom d'utilisateur et le mot de passe à CA EEM. CA EEM renvoie les données d'authentification et d'autorisation à CA Process Automation.

- Mode FIPS activé :
  - Les données transférées sont chiffrées avec l'algorithme SHA1, pris en charge par FIPS.
  - Un certificat PAM.cer est utilisé.
- Mode FIPS désactivé :
  - Les données transférées sont chiffrées avec l'algorithme MD5.
  - Un certificat PAM.p12 est utilisé.

Définition du type de configuration de CA EEM pour le stockage d'utilisateurs globaux

Si vous appliquez les conditions préalables requises de CA EEM pour l'installation initiale de CA Process Automation, tenez compte de ce qui suit :

- Los de la configuration de CA EEM, vous devez choisir de stocker les informations d'identification d'utilisateurs de manière interne ou de référencer ces informations à partir d'un annuaire externe ou de SiteMinder.



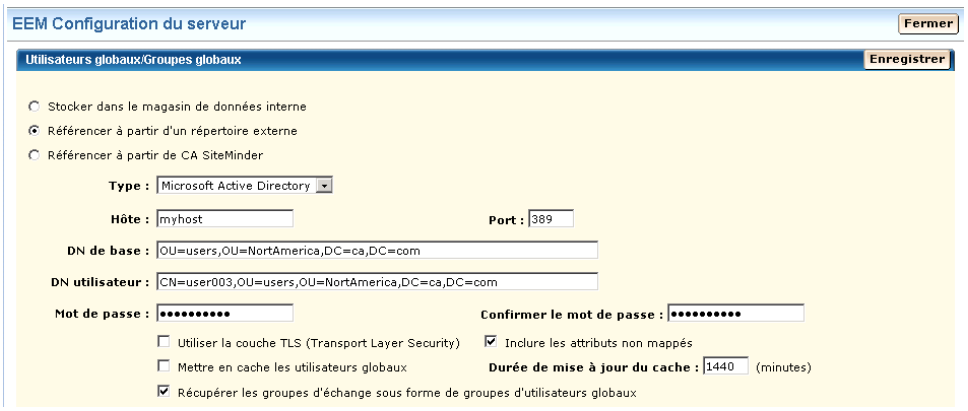
- Si vous utilisez une version de CA EEM existante qui prend en charge d'autres applications que CA Process Automation, cette option et le type de configuration est déjà défini. Toutes les applications utilisent le même type de configuration. Les types de configuration varient selon la version.
  - L'option Référencer à partir d'un annuaire externe de CA EEM 8.4 inclut le type de configuration de Microsoft Active Directory.
  - L'option Référencer à partir d'un annuaire externe de CA EEM 12.5 inclut son propre ensemble de types de configuration, y compris plusieurs domaines Active Directory et une forêt Active Directory.
- Si vous utilisez une nouvelle instance de CA EEM, tenez compte de la procédure suivante :
  1. Installez CA EEM et démarrez-le.
  2. Installez CA Process Automation. Lors de l'installation, enregistrez le produit dans CA EEM pour créer l'application CA Process Automation dans CA EEM et ignorez le test de connectivité à CA EEM.
  3. Connectez-vous à CA EEM avec les informations d'identification de l'utilisateur EiamAdmin et le nom de l'application CA Process Automation.
  4. Définissez le référentiel d'utilisateurs et, si vous sélectionnez Référencer à partir d'un annuaire externe, définissez les détails.

     Pour plus d'informations sur la configuration des utilisateurs globaux à partir d'un référentiel d'utilisateurs référencé dans CA EEM, consultez la documentation de CA EEM. Consultez également les exemples suivants :
     - Référencement d'utilisateurs globaux et de groupes globaux à partir de Microsoft Active Directory (page 91) (CA EEM r8.4)
     - Référencement d'utilisateurs globaux à partir de plusieurs domaines Microsoft Active Directory (CA EEM r12.5) (page 91)
  5. Lorsque vous êtes connecté à CA EEM, configurez des utilisateurs CA Process Automation. Consultez la section Affectation d'un groupe d'applications à un utilisateur global du *Manuel de l'administrateur de contenu*.
  6. Vous pouvez également configurer CA EEM pour permettre aux utilisateurs référencés de se connecter avec leur courriel (page 132).

Référencement d'utilisateurs globaux à partir de Microsoft Active Directory (CA EEM r8.4)

Lors de l'installation de CA EEM r8.4, vous pouvez sélectionner l'option Référencer à partir d'un annuaire LDAP externe, puis le type Microsoft Active Directory.

Lorsque vous utilisez le gestionnaire de réseau local Windows NT à des fins de sécurité, cochez la case Récupérer les groupes d'échange sous forme de groupes d'utilisateurs globaux, comme dans l'exemple suivant :



Lorsque vous enregistrez la configuration, les messages de statut suivants s'affichent :

- La liaison au répertoire externe a réussi.
- Les données du répertoire externe sont chargées.

Si l'authentification NTLM est activée et qu'un utilisateur global se connecte pour la première fois, une boîte de dialogue Authentification requise s'ouvre. CA EEM utilise le protocole NTLM pour authentifier les utilisateurs.

Référencement d'utilisateurs globaux à partir de plusieurs domaines Microsoft Active Directory (CA EEM r12.5)

Lors de l'installation de CA EEM r12.51, vous pouvez configurer CA EEM pour référencer plusieurs annuaires Microsoft Active Directory ou une forêt Active Directory.

Procédez comme suit :

1. Connectez-vous à CA EEM en tant qu'utilisateur EiamAdmin. Spécifiez <Global> pour l'application.
2. Cliquez sur l'onglet Configurer, puis sur Référentiel d'utilisateurs.
3. Dans la palette Référentiel d'utilisateurs, sélectionnez Référentiel d'utilisateurs.
4. Dans le champ Utilisateurs globaux/Groupes globaux, sélectionnez Référencer à partir d'un annuaire LDAP externe.

5. Dans la liste déroulante Type de configuration, sélectionnez Plusieurs domaines Microsoft Active Directory.
6. Cliquez sur Ajouter un répertoire et entrez le nom du premier domaine Active Directory dans le champ Nom.
7. Sous Paramètres du domaine, entrez le domaine dans le champ Domaine.
8. Entrez le nom d'hôte et le numéro de port dans les champs Hôte et Port, puis cliquez sur la flèche vers la droite.

   La liste Noms d'hôtes sélectionnés spécifie l'emplacement du domaine Active Directory.
9. Dans la liste déroulante Protocole, sélectionnez le protocole dont vous avez besoin.
10. Pour Nom unique de base, entrez une valeur sans espaces. La valeur spécifie l'annuaire LDAP externe qui contient des données pour des utilisateurs globaux et des groupes globaux. Dans l'exemple suivant, la valeur de OU= limite les groupes globaux chargés à ceux qui se trouvent dans l'unité organisationnelle spécifiée.

    ```
    OU=myorganizationalunit,DC=foo,DC=com
    ```
11. Spécifiez les informations d'identification que CA EEM doit utiliser pour accéder au domaine ou à l'unité organisationnelle spécifiée. Cet utilisateur doit être membre du domaine et de l'unité organisationnelle spécifiée pour le nom unique de base.
    a. Pour Nom unique de l'utilisateur, entrez le nom commun de l'utilisateur pour établir la connexion à l'annuaire LDAP externe. Utilisez le caractère d'échappement (\) avant les virgules entre les parties du nom commun. Par exemple :

       ```
       CN=firstname\,lastname,DC=foo,DC=com
       ```
    b. Entrez le mot de passe associé au nom commun spécifié pour le nom unique de l'utilisateur dans Mot de passe de l'utilisateur et Confirmer le mot de passe.
12. Spécifiez des valeurs pour la configuration avancée ou acceptez les valeurs par défaut.
13. Répétez les étapes 6 à 12 pour chaque domaine Active Directory à référencer.
14. Cliquez sur Enregistrer.

    Lorsque vous enregistrez la configuration, les messages de statut suivants s'affichent :

    - La liaison au répertoire externe a réussi.
    - Les données du répertoire externe sont chargées.

Conditions préalables la planification des ports

Les ports sont configurés pendant l'installation. Lors de la configuration des ports réseau, acceptez les valeurs par défaut sauf dans les cas suivants :

- Le port par défaut est utilisé par une autre application sur l'hôte.
- Une restriction de pare-feu empêche la communication sur le port par défaut.

Révisez l'utilisation des ports dans la rubrique Ports utilisés par CA Process Automation (page 227) et définissez les ports de remplacement pour tous les ports utilisés dans votre réseau ou sur l'hôte applicable. A l'exception du port pour les agents et pour CA EEM, toutes les autres propriétés sont stockées dans le fichier OasisConfig.properties dans *répertoire_installation*/server/c2o/.config. Si un conflit se produit après l'installation, vous pouvez modifier ce fichier manuellement.

Installation interactive de l'orchestrateur de domaine

L'installation de l'orchestrateur de domaine CA Process Automation requiert la présence de plusieurs composants, c'est pourquoi l'installation de CA Process Automation se compose essentiellement de deux phases :

1. Installation du logiciel tiers
2. Installation de l'orchestrateur de domaine

Les deux étapes doivent être effectuées lors de l'installant, de la réinstallant ou de la mise à niveau de CA Process Automation.

Vous pouvez effectuer l'installation à partir d'un média physique, d'une copie que vous réalisez du média physique ou que vous obtenez par téléchargement.

Vous pouvez quitter le processus d'installation à tout moment. Si vous l'annulez, une fenêtre contextuelle de confirmation s'affiche. Si vous confirmez l'annulation, les modifications que vous avez effectuées au cours des étapes d'installation sont ignorées.

Si vous avez un équilibreur de charge, il est recommandé de configurer l'orchestrateur de domaine sous la forme d'un orchestrateur mis en cluster, même si vous ne voulez pas le mettre en cluster immédiatement. Si vous décidez de le mettre en cluster ultérieurement sans l'avoir configuré comme un orchestrateur de domaine mis en cluster, vous devrez réinstaller l'orchestrateur de domaine pour permettre la prise en charge du cluster. Pour plus d'informations, consultez les rubriques :

- Conditions requises pour l'équilibreur de charge NGINX (page 36)
- Conditions requises pour l'équilibreur de charge F5 (page 53)
- Conditions requises pour l'équilibreur de charge Apache (page 261)

Les installations ultérieures requièrent la configuration de certaines valeurs lors de l'installation de l'orchestrateur de domaine. Par exemple, vous devez saisir de nouveau certains mots de passe pendant la mise à niveau ou l'installation d'autres orchestrateurs. Une façon simple de conserver un enregistrement des valeurs que vous avez entrées consiste à définir un plan pour les mots de passe avant de lancer l'installation interactive. Par exemple, enregistrez les mots de passe pour les éléments de serveur de base de données suivants.

- Certificat CA Process Automation
- Certificat CA EEM
- Base de données de référentiel
- Base de données de reporting
- Base de données d'exécution
- Administrateur de CA EEM

Informations complémentaires :

Installation autonome de l'orchestrateur de domaine (page 118)

Installation du logiciel Third-Party

Pour commencer l'installation de CA Process Automation, installez le logiciel tiers. A l'issue de cette installation, celle de l'orchestrateur se lance automatiquement.

Procédez comme suit :

1. Insérez le DVD1 du média d'installation de CA Process Automation dans un lecteur. Vous pouvez également accéder à l'emplacement dans lequel sont copiés les dossiers DVD1 et DVD2 contenant les fichiers d'installation.
2. Exécutez le programme d'installation approprié pour votre plate-forme et votre média :
   - **Windows :** Domain_Installer_windows.bat
   - **Linux ou UNIX :** Domain_Installer_unix.sh

   Ces fichiers appellent le programme d'installation tiers, puis le programme d'installation de l'orchestrateur de domaine.
3. Dans la boîte de dialogue Sélection de la langue, sélectionnez la langue préférée

   (langue par défaut). Indépendamment de la langue sélectionnée, CA Process Automation est installé avec prise en charge de toutes les localisations disponibles.

   La page Bienvenue dans l'assistant de configuration du programme d'installation de composants tiers CA Process Automation s'affiche.
4. Cliquez sur Suivant pour lancer l'installation des composants tiers.

5. Lisez le contrat de licence. Pour l'accepter, sélectionnez J'accepte les termes de ce contrat de licence et cliquez sur Suivant.
6. Pour installer les composants dans le répertoire de destination par défaut, cliquez sur Suivant, ou accédez à un autre répertoire et cliquez sur Suivant.

   Le programme d'installation crée le dossier automatiquement s'il n'existe pas. Un espace disque minimum de 8 Go est requis.

   Important : Vérifiez que la structure de répertoires CA Process Automation de l'emplacement d'installation ne dépasse pas 255 caractères. CA Technologies recommande de ne pas conserver plus de 64 caractères pour l'emplacement d'installation (*répertoire_installation)*.

   La liste des conditions requises tierces s'affiche. Les conditions préalables tierces pour l'orchestrateur de domaine incluent l'installation de JBoss, d'Hibernate et du fichier .jar du pilote JDBC. Dans CA Process Automation r 4.2, le service de messagerie ActiveMQ est utilisé avec JBoss 5.1.
7. Cliquez sur Suivant, puis surveillez l'installation de JBoss et des composants tiers.

   La fenêtre d'installation du fichier JAR de JDBC s'affiche.

8. Sélectionnez une ou plusieurs applications de serveur de base de données à utiliser pour l'accès interne aux bases de données CA Process Automation et spécifiez le chemin d'accès au fichier JAR du pilote JDBC approprié, Cliquez sur Suivant.

   - MySQL : accédez au fichier JAR de pilote JDBC que vous avez préalablement téléchargé vers MySQL. Exemple :

     `...votre_répertoire\mysql-connector-java-5.1.19-bin.jar`

   - MS SQL : acceptez le chemin d'accès par défaut au fichier JAR de JTDS JDBC sur le disque d'installation DVD1. Exemple :

     `...\DVD1\drivers\jtds-1.3.jar`

     (vous pouvez également accéder à un fichier JAR de JDBC différent),

   - Oracle : acceptez le chemin d'accès par défaut au fichier JAR de JDBC sur le disque d'installation DVD1. Exemple :

     `...DVD1\drivers\ojdbc14.jar`

     (vous pouvez également accéder à un fichier JAR de JDBC différent),

   Remarque : Vous devez spécifier un ou plusieurs pilotes JDBC. Il n'est généralement pas nécessaire de spécifier plusieurs pilotes JDBC pour la communication interne. Lors de l'installation de l'orchestrateur de domaine, vous pouvez installer des pilotes JDBC supplémentaires en vue de leur utilisation par d'autres orchestrateurs ou agents avec les opérateurs de base de données (précédemment module JDBC).

9. Lorsque la fenêtre Fin de l'assistant d'installation de CA Process Automation s'affiche, insérez le DVD 2 d'installation de CA Process Automation ou remplacez DVD1 par DVD2 dans le champ. Vous pouvez également accédez au répertoire qui contient les fichiers du média d'installation DVD2. Cliquez sur Terminer.

   Le programme d'installation de logiciels tiers transfère le contrôle au programme d'installation de l'orchestrateur de domaine CA Process Automation. Un délai peut survenir entre la fermeture de l'interface utilisateur du programme d'installation de composants tiers et l'ouverture de l'interface utilisateur pour l'installation du domaine CA Process Automation. Il ne s'agit pas d'une erreur ou d'un problème.

Installation de l'orchestrateur de domaine

Une fois les composants tiers installés par le programme d'installation tiers, ce dernier copie les fichiers d'installation CA Process Automation dans l'hôte et démarre le programme d'installation de l'orchestrateur de domaine.

Cette section décrit l'installation d'un orchestrateur de domaine non mis en cluster ou du premier noeud d'un orchestrateur de domaine mis en cluster.

Procédez comme suit :

1. Sur la page de bienvenue, cliquez sur Suivant.
2. Acceptez le contrat de licence et cliquez sur Suivant.

3. Vérifiez que le chemin d'accès affiché pointe vers le répertoire de base Java. Si le chemin d'accès au répertoire de base Java n'est pas affiché, procédez comme suit :
   a. Cliquez sur Parcourir.
   b. Accédez à l'emplacement correct.
   c. Sélectionnez le kit de développement Java à utiliser. Par exemple, sélectionnez :

      ```
      C:\Program Files\Java\jdk1.7.0_21
      ```

   d. Cliquez sur Suivant.

   Le JDK est validé.
4. Surveillez la progression de la copie des fichiers.
5. Pour configurer CA Process Automation de façon à l'utiliser avec CA SiteMinder, vérifiez que toutes les conditions préalables de CA SiteMinder sont remplies. Dans la fenêtre de configuration du domaine de CA Process Automation, remplissez les champs suivants :

   Configurer l'authentification unique

   Cochez cette case pour configurer CA SiteMinder avec l'orchestrateur de domaine.

   Vérifiez que l'agent Web CA SiteMinder est configuré avec le même équilibreur de charge Apache que vous utilisez pour CA Process Automation.

   Type d'authentification unique

   Une fois CA SiteMinder configuré, sélectionnez le type d'authentification **En-Tête**.

   Le type d'authentification détermine comment CA Process Automation est informé de l'ID d'utilisateur lorsqu'un utilisateur est connecté via CA SiteMinder. Les utilisateurs peuvent sélectionner les valeurs par défaut de la liste Type d'authentification unique.

   Paramètres d'authentification unique

   Définit le nom du paramètre d'authentification lorsque CA SiteMinder est configuré.

   Acceptez les valeurs par défaut ou entrez de nouvelles valeurs selon votre configuration de CA SiteMinder.

   - Sélectionnez **sm_user** comme paramètre d'authentification unique pour IIS.
   - Sélectionnez **SM_User** comme paramètre d'authentification unique pour Apache.

   Type de serveur

   Spécifie le type d'installation Nouvel orchestrateur.

6. Effectuez l'action appropriée :

   - Si vous envisagez de configurer un orchestrateur de domaine mis en cluster, lisez les instructions et remplissez la fenêtre Configuration.
   - Si vous configurez l'orchestrateur de domaine en vue d'une utilisation avec CA SiteMinder, lisez les instructions et remplissez la fenêtre Configuration.

   Configurer l'équilibreur de charge

   Permet d'activer la mise en cluster au niveau de l'orchestrateur de domaine à installer.

   Option activée

   Activez la mise en cluster au niveau de l'orchestrateur de domaine à installer. Avant de sélectionner cette option, vérifiez que les conditions requises pour l'équilibreur de charge NGINX (page 35) ou pour l'équilibreur de charge F5 (page 53) sont remplies.

   Option désactivée

   Désactivez la mise en cluster au niveau de l'orchestrateur de domaine à installer.

   Noeud de travail de l'équilibreur de charge

   Définit le nom du noeud de travail de l'équilibreur de charge. La première installation de l'orchestrateur de domaine est le premier noeud dans le cluster. Sa valeur est donc généralement node1.

   Si votre équilibreur de charge est de type Apache, votre entrée doit correspondre au nom du noeud dans la variable worker.*nom_noeud*.host associée à l'hôte dans le fichier *répertoire_installation_apache*\conf\workers.properties d'Apache. Dans l'exemple suivant, la valeur de la variable, **node1**, est la valeur à affecter.

   `worker.`**`node1`**`.host=`*`DomainOrchestratorHostName`*

   Si le fichier workers.properties spécifie worker.**abc**.host, saisissez **abc**.

   Si votre équilibreur de charge est de type F5, acceptez les valeurs par défaut. La valeur des noeuds de travailleur n'est pas pertinente pour F5. Il n'y a donc aucun lien aux conditions requises que vous avez remplies pour F5.

   Valeur par défaut : node1. Les caractères spéciaux, y compris les traits d'union, ne sont pas pris en charge.

Nom d'hôte public

Spécifie le nom d'hôte public pour le serveur Apache, NGINX ou F5. Exemple :

`loadbalancerhost.mycompany.com`

- Si vous avez coché la case Configurer l'authentification unique, définissez ce champ sur le nom de domaine complet du serveur IIS/Apache sur lequel l'agent Web CA SiteMinder est configuré.
- Si vous avez coché la case Configurer l'équilibreur de charge sans sélectionner l'option Configurer l'authentification unique, définissez ce champ sur le nom de domaine complet de l'équilibreur de charge Apache, NGINX ou F5.

Numéro de port d'hôte public

Définit le port HTTP pour IIS/Apache (hôte public) ou l'hôte F5 si la case Prise en charge des communications sécurisées est décochée.

Si vous modifiez cette valeur lors de l'installation et de la configuration de l'équilibreur de charge Apache, F5 ou NGINX, mettez à jour cette valeur en conséquence. Ce port et le nom de l'hôte public sont utilisés pour accéder à CA Process Automation. Exemple :

`http://nom_hôte_public:80/itpam`

Valeur par défaut : 80

Port d'hôte public sécurisé

Définit le port HTTPS pour l'hôte public spécifié si la case Prise en charge des communications sécurisées est cochée.

Ce port fait partie de l'URL qui permet d'accéder aux services Web CA Process Automation. Ce port et le nom de l'hôte public sont utilisés pour accéder à CA Process Automation. Exemple :

`https://nom_hôte_public:443/itpam`

Valeur par défaut : 443

Prise en charge des communications sécurisées

Indique si l'équilibreur de charge (F5, NGINX ou Apache) utilise le protocole HTTPS pour les communications sécurisées.

Option activée

Indique qu'IIS ou Apache (hôte public) utilise HTTPS pour communiquer.

Remarque : Si vous avez effectué les étapes de configuration de la communication sécurisée pour Apache, sélectionnez cette option.

Indique que F5 utilise le protocole HTTPS pour communiquer.

Option désactivée

Indique qu'IIS ou Apache (hôte public) utilise HTTP pour communiquer.

Indique que F5 utilise le protocole HTTP pour communiquer.

7. Cliquez sur Suivant.
8. Dans le champ Société, saisissez votre nom de société, puis cliquez sur Suivant.

   Quand vous cliquez sur Aide, A propos de, CA Process Automation affiche votre entrée comme valeur pour Licence d'utilisation du produit accordée à.
9. Saisissez un mot de passe de certificat, puis ressaisissez-le pour le confirmer et cliquez sur Suivant.

   Mot de passe du certificat

   Définit le mot de passe de contrôle de l'accès aux clés de chiffrement des mots de passe et autres données critiques. Utilisez ce mot de passe quand vous installez un autre orchestrateur ou quand vous ajoutez des noeuds de cluster à un orchestrateur. Le mot de passe du certificat est propre à un domaine CA Process Automation unique.

   Confirmer le mot de passe du certificat

   Fait correspondre votre entrée dans ce champ avec votre entrée dans le champ Mot de passe du certificat pour vérifier le mot de passe.

   Important : Dans la page Définir le mot de passe de certificat, avant de cliquer sur Suivant, enregistrez votre mot de passe de certificat dans un emplacement sécurisé pour pouvoir vous y référer ultérieurement. Ce même mot de passe de certificat est requis lors de la mise à niveau de l'orchestrateur de domaine et d'autres orchestrateurs (y compris des noeuds de cluster) vers une nouvelle version.

10. (Windows uniquement) Spécifiez les préférences suivantes pour le menu Démarrer, puis cliquez sur Suivant.

    [Nom du dossier du menu Démarrer]

    Définit le nom du dossier du menu Démarrer CA Process Automation si vous avez décoché la case Ne pas créer de dossier dans le menu Démarrer. Acceptez la valeur par défaut ou saisissez le nom du dossier du menu Démarrer pour CA Process Automation.

    Valeur par défaut : CA Process Automation 4.0

    Créer des raccourcis pour tous les utilisateurs

    Spécifie si le nom du dossier du menu de raccourcis spécifié doit être affiché pour tous les utilisateurs qui se connectent au serveur à l'aide de l'orchestrateur de domaine CA Process Automation.

    Option activée : affiche les raccourcis.

    Option désactivée : n'affiche pas les raccourcis.

    Ne pas créer de dossier dans le menu Démarrer

    Spécifie si une entrée CA Process Automation doit être créée dans le menu Démarrer.

    Option activée : créez une entrée de menu Démarrer pour CA Process Automation.

    Option désactivée : ne créez pas d'entrée de menu Démarrer pour CA Process Automation.

11. Remplissez les champs suivants pour définir le mode de communication de l'orchestrateur de domaine avec d'autres composants CA Process Automation et applications, puis cliquez sur Suivant.

    Hôte de serveur

    Définit l'une des propriétés suivantes :

    - Nom d'hôte ou adresse IP du système hôte sur lequel l'orchestrateur de domaine est déployé.
    - Un alias de DNS qui renvoie le système hôte.

    Nom d'affichage

    Spécifie le nom de l'orchestrateur de domaine affiché dans l'explorateur de configurations CA Process Automation.

    - Si vous ne configurez pas d'équilibreur de charge, le nom d'affichage correspond au nom d'hôte du serveur.
    - Si vous configurez un équilibreur de charge, le nom d'affichage correspond au nom de domaine complet du serveur sur lequel l'équilibreur de charge est installé.

Prise en charge des communications sécurisées

Spécifie si la communication avec CA Process Automation doit être sécurisée, par opposition à la communication de base standard. Cette valeur permet d'indiquer si le port activé est de type HTTP ou HTTPS.

Option activée : utilisez le protocole HTTPS pour les communications.

Option désactivée : n'utilisez pas le protocole HTTPS pour les communications Utilisez HTTP à la place.

Port du serveur

Spécifie le port que l'orchestrateur de domaine utilise pour communiquer avec d'autres orchestrateurs et agents.

Valeur par défaut : 80 pour les connexions de base HTTP ou 443 pour les connexions sécurisées HTTPS.

Port HTTP

Définit le port HTTP utilisé pour le serveur Web si la case Prise en charge des communications sécurisées est décochée.

Remarque : Ce port est indiqué dans l'URL utilisée pour accéder aux services Web CA Process Automation et à la fenêtre de connexion à CA Process Automation.

Valeur par défaut : 8080

Port HTTPS

Lorsque vous sélectionnez Prise en charge des communications sécurisées, ce champ spécifie le port utilisé dans l'URL qui accède aux services Web CA Process Automation et à l'interface utilisateur CA Process Automation basée sur un navigateur.

Valeur par défaut : 8443

Remarque : Pour pouvoir saisir une valeur dans ce champ, activez l'option Prise en charge des communications sécurisées.

Port JNDI

Définit le port du serveur d'attribution de noms Java que le serveur Web utilise.

Remarque : N'accédez pas à ce port hors de ce système hôte.

Valeur par défaut : 1099

Port RMI

Définit le port RMI que le serveur Web utilise.

Remarque : N'accédez pas à ce port hors de ce système hôte.

Valeur par défaut : 1098

Port SNMP

Spécifie le port d'écoute d'interruption SNMP pour CA Process Automation.

Valeur par défaut : 162

12. Acceptez le chemin d'accès par défaut ou accédez à un répertoire temporaire dans lequel les scripts sont exécutés. Cliquez sur Suivant.

    Ce répertoire doit être accessible en écriture par tous les utilisateurs.

13. Remplissez les champs suivants pour définir des paramètres PowerShell, puis cliquez sur Suivant.

    Définir la politique d'exécution PowerShell

    Spécifie si PowerShell doit être utilisé ou non.

    Option activée : activez l'utilisation de PowerShell et définissez la politique d'exécution PowerShell au niveau du chemin d'accès spécifié sur RemoteSigned.

    Option désactivée : n'activez pas l'utilisation de PowerShell.

    Chemin d'accès à PowerShell sur l'ordinateur hôte

    CA Process Automation détecte automatiquement le chemin d'accès PowerShell.

    Remarque : Lorsque vous cliquez sur Suivant, le programme d'installation valide le chemin d'accès PowerShell fourni.

14. Définissez les paramètres de sécurité de CA EEM. L'ordre dans lequel les champs sont présentés dans cette étape dérive des dépendances plutôt que de l'ordre des champs affiché dans l'interface utilisateur.

    a. Complétez les champs requis suivants :

    Serveur EEM

    Définit le nom de domaine complet du serveur CA EEM que CA Process Automation utilise pour authentifier et autoriser les utilisateurs CA Process Automation. Si vous configurez EEM pour la haute disponibilité, vous pouvez également définir un serveur CA EEM de sauvegarde. Utilisez une virgule comme délimiteur des noms de serveur.

    Nom de l'application EEM

    Définit le nom de l'application CA Process Automation affiché dans CA EEM. Si vous utilisez le même serveur CA EEM avec plusieurs domaines CA Process Automation, chaque domaine CA EEM doit porter un nom d'application EEM unique. Le nom que vous entrez ici s'affiche dans la liste déroulante de la page de connexion du serveur CA EEM.

    Si vous procédez à la mise à niveau, ce champ est déjà rempli avec la valeur utilisée lors de l'installation initiale. Cette valeur préserve les affectations de groupe d'utilisateurs, les politiques personnalisées et les groupes personnalisés de CA EEM. CA EEM utilise cette valeur pour identifier le domaine CA Process Automation.

    Valeur par défaut : Process Automation

    Utiliser le certificat conforme à la norme FIPS

    Spécifie si des certificats conformes à la norme FIPS doivent être utilisés. Ce paramètre doit correspondre à la configuration du mode FIPS de CA EEM.

    Remarque : Pour déterminer la configuration du mode FIPS de CA EEM, cliquez sur A propos de dans CA EEM. Les caractéristiques du produit incluent la désactivation ou l'activation de la compatibilité avec la norme FIPS.

    Option sélectionnée : le mode FIPS est défini sur Activé dans CA EEM.

    Option désélectionnée : le mode FIPS est défini sur Désactivé dans CA EEM.

b. Une fois la page renseignée, spécifiez que vous *voulez enregistrer* le nom de l'application spécifié pour ce domaine CA Process Automation dans CA EEM. Le processus d'enregistrement génère des certificats conformes à la norme FIPS ou des certificats non conformes à la norme FIPS, en fonction de votre sélection. Cette case à cocher s'affiche au-dessus du bouton Enregistrer. La sélection de cette option correspond à la configuration standard.

Enregistrer l'application dans CA EEM

Spécifie si la valeur de Nom de l'application EEM doit être enregistrée pour CA Process Automation dans CA EEM et génère le certificat que CA Process Automation utilise pour se connecter à son application dans le serveur CA EEM. Le kit de développement logiciel de CA EEM gère la connexion. Si vous y êtes invité, indiquez que vous voulez mettre à niveau l'application CA Process Automation dans CA EEM.

Option activée : active le bouton Enregistrer. Reportez-vous à l'étape 16. Désactive le champ Fichier de certificat EEM. Pour une nouvelle installation d'orchestrateur de domaine, cochez cette case systématiquement. Une fois les champs de paramètres de sécurité EEM remplis, cliquez sur Enregistrer.

Option désactivée : désactive le bouton Enregistrer. Active le champ Fichier de certificat EEM.

c. Pour une nouvelle installation, remplissez le champ suivant uniquement si vous n'enregistrez pas l'application dans CA EEM. Cliquez sur Parcourir et accédez à l'emplacement du fichier de certificat. Une fois que le fichier de certificat est chargé, le programme d'installation le place dans le répertoire suivant :

`répertoire_installation/server/c2o/.c2orepository/public/certification`

Remarque : Si vous procédez à la mise à niveau, ce champ est automatiquement rempli avec le chemin d'accès au fichier de certificat.

Fichier de certificat EEM

Définit le fichier de certificat CA EEM à utiliser pour CA Process Automation. Vous pouvez généralement accepter la valeur par défaut.

Valeurs par défaut :

PAM.cer si vous avez coché la case Utiliser le certificat conforme à la norme FIPS.

PAM.pem si vous avez décoché la case Utiliser le certificat conforme à la norme FIPS.

d. Remplissez l'un des champs suivants, si requis.

Fichier de clé de certificat

Le cas échéant (reportez-vous aux remarques), cliquez sur Parcourir et recherchez l'emplacement de la clé de certificat, par exemple, le fichier PAM.key. Une fois que le fichier de certificat est chargé, le programme d'installation le place dans le répertoire suivant :

répertoire_installation/server/c2o/.c2orepository/public/certification

Remarques :

- S'il s'agit d'une nouvelle installation, ce champ n'est pas requis si vous utilisez le mode FIPS et que vous tentez d'effectuer un enregistrement. Le processus d'enregistrement génère le fichier de clé de certificat avec le certificat.
- S'il s'agit d'une nouvelle installation, ce champ est requis si vous utilisez le mode FIPS sans tentative d'enregistrement.
- Si vous procédez à la mise à niveau, ce champ est rempli avec le chemin d'accès au fichier de clé.

Mot de passe du certificat EEM

Obligatoire si vous n'utilisez pas la norme FIPS. Définit le mot de passe du certificat CA EEM. Ce mot de passe protège le certificat PAM.p12. CA Process Automation s'en sert pour ouvrir et utiliser le certificat PAM.p12.

e. Remplissez les champs suivants uniquement si vous configurez CA EEM pour référencer des utilisateurs à partir d'un annuaire LDAP externe. Dans le cas contraire, ignorez cette étape.

Domaine Active Directory par défaut

(Applicable uniquement si vous prévoyez de référencer plusieurs domaines Active Directory lors de configuration de CA EEM r12.51. Reportez-vous à l'étape 17.) Spécifie le domaine Active Directory à utiliser en tant que domaine par défaut. Les utilisateurs de CA Process Automation appartenant au domaine spécifié peuvent se connecter à CA Process Automation avec leur nom d'utilisateur non qualifié. Les utilisateurs appartenant à d'autres domaines Active Directory doivent spécifier leur nom principal (*domaine**nom_utilisateur* ou *nom_utilisateur@domaine*) et leur mot de passe lorsqu'ils se connectent à CA Process Automation. La valeur saisie doit correspondre à l'entrée du champ Domaine pour l'un des domaines Active Directory que vous configurez pour le référentiel d'utilisateurs référencé par CA EEM.

CA EEM doit être convenablement configuré pour pouvoir authentifier le format nom_utilisateur@domaine du nom principal.

Remarque : Consultez la rubrique Configuration de CA EEM pour permettre aux utilisateurs référencés de se connecter avec une adresse électronique (page 132).

Activer l'authentification directe NTLM

Spécifie si CA EEM utilise le protocole NTLM pour authentifier les utilisateurs CA Process Automation.

Option activée : active l'authentification directe NTLM. CA EEM utilise le protocole NTLM pour authentifier les utilisateurs qui accèdent à CA Process Automation.

Option désactivée : désactive l'authentification directe NTLM. Les utilisateurs qui accèdent à CA Process Automation doivent entrer des informations d'identification dans la boîte de dialogue de connexion de CA Process Automation. CA EEM valide les informations d'identification avec les annuaires Microsoft Active Directory référencés pour authentifier les utilisateurs.

15. Enregistrez la valeur de Nom de l'application EEM configurée avec CA EEM ou ignorez l'enregistrement. Le processus d'enregistrement génère les certificats CA Process Automation selon la longueur requise.

    - Dans le cas d'une nouvelle installation, cliquez sur Enregistrer, remplissez les champs suivants dans la fenêtre Informations d'identification EEM et cliquez sur OK. Lorsque le message Application enregistrée s'affiche, cliquez sur OK.

      Nom de l'administrateur EEM

      Définit le nom de l'administrateur CA EEM. Entrez **EiamAdmin**.

      Mot de passe de l'administrateur EEM

      Définit le mot de passe du compte d'utilisateur EiamAdmin. Si vous avez installé CA EEM, entrez le mot de passe que vous avez créé pour l'utilisateur EiamAdmin. Dans le cas contraire, contactez l'administrateur CA EEM pour obtenir le mot de passe.

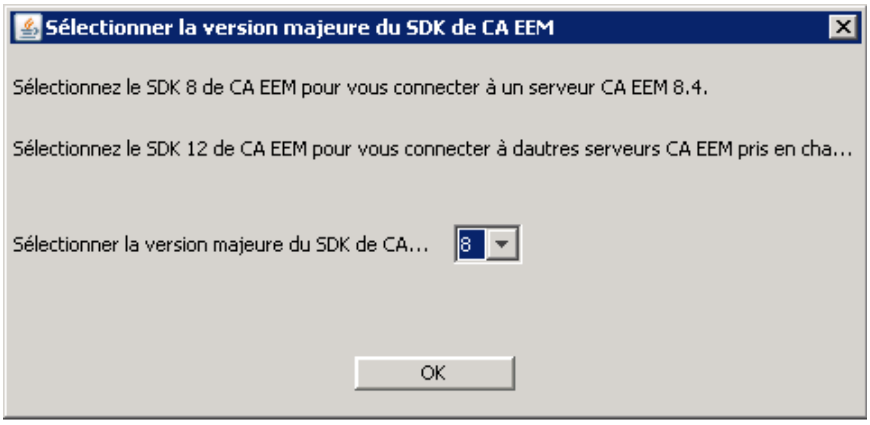
    - Si vous utilisez des certificats FIPS, les nouveaux certificats PAM.cer et PAM.key écrasent les certificats existants, le cas échéant. Si vous n'utilisez aucun certificat FIPS, le nouveau certificat PAM.p12 écrase le certificat existant dans CA Process Automation, le cas échéant. Ce certificat est protégé par le mot de passe entré dans le champ Mot de passe du certificat EEM. Le champ Fichier de certificat EEM est rempli avec un chemin d'accès au fichier similaire à :

      `répertoire_installation/server/c2o/.c2orepository/public/certification/PAM.p12`

      Remarque : Les certificats ne sont pas régénérés si vous êtes invité à mettre à niveau l'application CA Process Automation dans CA Embedded Entitlements Manager et que vous choisissez de ne *pas* le mettre à niveau.

La liste à puces suivante décrit les scénarios d'utilisation :

- Nouvelle installation avec enregistrement : le processus d'installation détecte la version du serveur CA EEM et sélectionne le kit de développement logiciel approprié.
- Nouvelle installation sans enregistrement : le processus d'installation vous invite à choisir un kit de développement logiciel en fonction de la version de compilation de CA EEM. Si vous ne connaissez pas la version de compilation du serveur CA EEM, connectez-vous à CA EEM et examinez les informations A propos de.


Sélectionner la version majeure du SDK de CA EEM
Sélectionnez le SDK 8 de CA EEM pour vous connecter à un serveur CA EEM 8.4.
Sélectionnez le SDK 12 de CA EEM pour vous connecter à dautres serveurs CA EEM pris en cha...
Sélectionner la version majeure du SDK de CA...
8
OK

16. (Facultatif) Si vous voulez tester les paramètres de CA EEM et que vous avez configuré CA EEM pour référencer à partir d'un annuaire externe, vous devez d'abord créer un utilisateur test. Un utilisateur test est un utilisateur que vous récupérez d'un domaine Active Directory de votre choix et que vous affectez au groupe PAMAdmins. Procédez comme suit :

    a. Accédez à CA EEM utilisé par CA Process Automation. Utilisez l'URL suivante :

       `https://nom_hôte:5250/spin/eiam`

       La boîte de dialogue CA Embedded Entitlements Manager s'ouvre.

    b. Dans la liste déroulante Application, sélectionnez le nom configuré dans le champ Nom de l'application EEM.

    c. Saisissez EiamAdmin et le mot de passe de l'administrateur de CA EEM que vous avez configuré.

    d. Cliquez sur Connexion.

    e. Cliquez sur l'onglet Gestion des identités.

    f. Sous Recherche d'utilisateurs, à l'endroit où Utilisateurs globaux est sélectionné, sélectionnez Nom ou Prénom et entrez la valeur appropriée dans le champ Valeur. Puis, cliquez sur OK. (les valeurs partielles sont acceptées).

       Votre nom s'affiche sous Utilisateurs dans le volet Utilisateurs.

    g. Double-cliquez sur votre nom pour afficher votre compte d'utilisateur chargé.

       Votre compte d'utilisateur inclut deux sections User Details (Détails de l'utilisateur). La section supérieure vous permet de définir un groupe pour votre rôle dans CA Process Automation. La section supérieure intitulée Informations sur les utilisateurs globaux, contient des informations de l'annuaire externe.

    h. Cliquez sur le bouton Add Application User Details (Ajouter les détails des utilisateurs de l'application) sous la section supérieure.

       La liste Groupes d'utilisateurs disponibles contient un groupe pour chacun rôle par défaut.

    i. Pour déplacer ce groupe vers la liste Utilisateurs/groupes sélectionnés, sélectionnez PAMAdmins et cliquez sur la flèche vers la droite.

    j. Cliquez sur Enregistrer.

    k. Cliquez sur Déconnexion.

17. (Facultatif) Testez les paramètres CA EEM. Lors de cette étape, vous devez entrer les informations d'identification d'un utilisateur défini dans CA EEM. Si vous utilisez CA EEM comme annuaire local (par défaut), vous pouvez entrer les informations d'identification de l'un des utilisateurs par défaut. Si CA EEM pointe vers un annuaire externe, saisissez vos propres informations d'identification (si vous avez terminé l'étape précédente).

    a. Cliquez sur Tester les paramètres EEM.

    b. Si vous utilisez CA EEM comme annuaire local et effectuez une nouvelle installation, saisissez pamadmin dans le champ Nom d'utilisateur et pamadmin dans le champ Mot de Passe, puis cliquez sur OK.

    c. Si vous utilisez un compte d'utilisateur référencé à partir d'un répertoire externe, saisissez les informations d'identification d'utilisateur définies dans le répertoire externe. Il s'agit du compte de l'utilisateur test créé à l'étape précédente.

    La fenêtre Vérifier les paramètres EEM affiche les champs suivants :

    Connexion

    Indique si vous pouvez établir une connexion au serveur CA EEM spécifié avec les valeurs fournies dans la fenêtre Paramètres CA EEM.

    Limites : OK et Non valide

    Remarque : Si la valeur indique Non valide, les champs suivants ne sont pas affichés.

    L'utilisateur indiqué appartient au groupe d'utilisateurs.

    Indique si vous pouvez authentifier l'utilisateur, c'est-à-dire, si la connexion est permise.

    Limites : OK et Non valide

    L'utilisateur est un administrateur.

    Indique si l'utilisateur a l'autorisation d'effectuer des tâches d'administrateur. Les membres du groupe PAMAdmins disposent de ces droits.

    Limites : Oui et Non

    Mise à niveau EEM

    Indique si le schéma d'application CA Process Automation du serveur EEM est mis à niveau. Si le message Aucune mise à niveau n'est requise s'affiche, cliquez sur OK.

    Remarque : Ce champ s'affiche uniquement si la valeur n'est pas définie sur OK. Si la valeur n'est pas définie sur OK, mettez à niveau l'instance.

18. Lorsque vous avez passé en revue les résultats, cliquez sur OK, puis sur Suivant.

19. Remplissez les champs suivants pour définir les paramètres de la base de données de bibliothèque (c'est-à-dire, de la base de données de référentiel).

Type de base de données

Spécifie le type de système de base de données. Sélectionnez un type pris en charge dans la liste déroulante.

Valeurs : MySQL, MS SQL et Oracle

Remarque : Si cette installation est utilisée dans un environnement de production, il est recommandé de sélectionner MS SQL ou Oracle. MySQL est le choix approprié pour les orchestrateurs de domaine sous charge légère.

Nom d'utilisateur

Spécifie un nom d'utilisateur autorisé à créer la base de données, et à y accéder, sur le serveur de base de données. Le compte doit posséder les autorisations de création de la base de données sur le serveur ou être propriétaire (DBO) d'une base de données existante. Les valeurs suivantes sont automatiquement remplies en fonction de la sélection de la base de données :

- MS SQL : **sa**
- MySQL : **root**

Mot de passe

Définit le mot de passe associé au nom d'utilisateur spécifié.

Serveur de base de données

Définit le nom d'hôte ou l'adresse IP du serveur de base de données.

- Si vous avez configuré le type de base de données MS SQL et que le serveur hôte comprend uniquement une instance SQL Server ou si vous avez sélectionné un autre type de base de données, spécifiez le nom d'hôte ou l'adresse IP du serveur de base de données. Ce nom est l'instance par défaut.
- Si vous avez configuré le type de base de données MS SQL et que le serveur hôte comprend plusieurs instances SQL Server, spécifiez l'instance nommée SQL Server. Utilisez le format hôte\instance : *dbserver.mycompany*.com*pamdb.*
- Si vous avez configuré le type de base de données Oracle, spécifiez un nom SID.

Port de base de données

Définit le port de connexion configuré sur le serveur de base de données.

- Pour MS SQL, le port par défaut est 1433.
- Pour MySQL, le port par défaut est 3306.
- Pour Oracle, le port par défaut est 1521.

Base de données de référentiel

Définit le nom de la base de données de stockage des objets de la bibliothèque et des autres données.

Chaque orchestrateur peut posséder sa propre base de données de référentiel ou de bibliothèque. Vous pouvez également partager la base de données de bibliothèque entre les orchestrateurs. Chaque base de données doit posséder un nom unique. Etudiez la possibilité de définir une convention d'attribution d'un nom pour vos bases de données CA Process Automation avec cette installation initiale.

Fichier JAR de pilote

Définit le fichier JAR du pilote JDBC pour le type de base de données spécifié. Le dossier de pilotes du dossier DVD1 du support d'installation fournit des pilotes par défaut pour les serveurs de base de données Microsoft SQL Server et Oracle.

Valeurs par défaut :

SQL Server : jtds-1.3.jar

Oracle : ojdbc14.jar

MySQL : cliquez sur Parcourir, puis accédez au fichier JAR que vous avez téléchargé (par exemple mysql-connector-java-5.1.18-bin.jar).

Classement de la base de données

Définit les règles de tri des données pour MS SQL et Oracle. Le respect de la casse, les marques d'accent, les types de caractère kana et la largeur de caractère peuvent faire partie de l'ensemble de règles. Ce champ est une liste déroulante. Il est recommandé d'accepter la valeur par défaut. Ce champ n'est pas applicable à MySQL.

Valeur par défaut : SQL_Latin1_General_CP1_CI_AS

Utiliser une chaîne de connexion

Cochez cette case pour fournir une chaîne de connexion et établir la connexion à la base de données Oracle.

Remarque : Cette case à cocher est activée pour la base de données Oracle uniquement.

Chaîne de connexion

Saisissez une chaîne de connexion JDBC dans l'un des formats suivants :

`jdbc:oracle:thin:`*`serveur_BdD`*`:`*`numéro_port`*`:`*`nom_BdD`*

`jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=`*`nom_hôte`*`)(PORT=`*`numéro_port`*`))(CONNECT_DATA=(SERVICE_NAME=`*`ID_service`*`)))`

20. Cliquez sur Tester les paramètres de la base de données pour tester la connectivité entre CA Process Automation et le serveur de base de données spécifié à l'aide du port de base de données et du fichier JAR spécifiés.

    Si un message indique que les bases de données sont absentes, fermez-le et cliquez sur Créer une base de données. Excepté avec Oracle, vous pouvez créer les bases de données requises par l'orchestrateur pendant l'installation.

    Créer une base de données

    Créez la base de données de référentiel si vous avez spécifié MS SQL ou MySQL.

    Remarque : Si vous utilisez un serveur de base de données Oracle, vous avez déjà créé la base de données de référentiel, puisque cette tâche préalable est requise au niveau du serveur de base de données.

    Un message indique qu'une base de données a été créée avec le nom que vous avez fourni. Cliquez sur OK. Cliquez sur Tester les paramètres de la base de données à nouveau.

21. Cliquez sur Suivant.

22. Entrez les informations relatives à la base de données d'exécution, manuellement ou en les copiant à partir des données que vous avez saisies concernant la base de données de référentiel. Si la base de données est de type MSSQL ou MySQL, cliquez sur Créer une base de données. Cliquez sur Tester les paramètres de la base de données,

    Seuls deux champs Base de données d'exécution ne sont pas identiques aux champs Paramètres de la base de données de référentiel (de bibliothèque). Pour accéder aux descriptions des autres champs, consultez l'étape 20.

    Copier à partir du référentiel principal

    Spécifie si les paramètres de la base de données de bibliothèque doivent être copiés dans la fenêtre des paramètres de la base de données d'exécution.

    Option activée : copie les paramètres de la base de données de bibliothèque dans cette boîte de dialogue. Cette option peut vous faire gagner du temps si vous utilisez le même serveur de base de données pour les deux bases de données CA Process Automation. Si vous sélectionnez cette option, saisissez le nom de la base de données d'exécution dans le champ Base de données d'exécution. Cliquez sur Tester les paramètres de la base de données, puis sur Créer une base de données.

    Option désactivée : ne copiez pas les paramètres de la base de données de bibliothèque dans cette boîte de dialogue. Cette option est appropriée si le type de base de données que vous utilisez pour les données d'exécution n'est pas le même que celui utilisé pour les enregistrements de bibliothèque.

    Base de données d'exécution

    Définit le nom de la base de données ou du schéma de stockage des instances d'exécution. Deux orchestrateurs ne peuvent pas pointer vers la même base de données d'exécution. Entrez un nom unique.

    Valeur par défaut : pam

    Important : Vous ne pouvez pas partager une base de données d'exécution entre plusieurs orchestrateurs. Si vous désinstallez puis réinstallez CA Process Automation, la base de données d'exécution que vous configurez ici ne change pas.

23. Cliquez sur Suivant.

24. Configurez la base de données de reporting de l'une des façons suivantes :

    - Si vous utilisez le même serveur de base de données pour la base de données de reporting et la base de données de référentiel :

        a. Saisissez un nom unique pour la base de données de reporting dans le champ Base de données de reporting.

        b. Cochez la case Copier à partir du référentiel principal pour entrer automatiquement les données partagées.

        c. Cliquez sur Tester les paramètres de la base de données,

        d. Si la base de données est de type MS SQL ou MySQL, cliquez sur Créer une base de données

    - Si vous utilisez un serveur de base de données différent pour la base de données de reporting et la base de données de référentiel :

        a. Saisissez un nom unique pour la base de données de reporting dans le champ Base de données de reporting.

        b. Décochez la case Copier à partir du référentiel principal.

        c. Sélectionnez le type de base de données dans la liste déroulante Type de base de données.

        d. Dans le champ Nom d'Utilisateur, entrez un nom d'utilisateur autorisé à créer la base de données et à y accéder sur le serveur de base de données (par exemple, saisissez sa pour MS SQL et root pour MySQL).

        e. Cliquez sur Tester les paramètres de la base de données,

        f. Si la base de données est de type MS SQL ou MySQL, cliquez sur Créer une base de données (ne cliquez pas sur ce bouton si la base de données de reporting est exécutée sur un serveur de base de données Oracle).

    Référez-vous aux descriptions de champs suivantes :

    Copier à partir du référentiel principal

    Permet de copier les paramètres de la base de données de bibliothèque dans la fenêtre des paramètres de la base de données de reporting. Seuls deux champs Base de données de reporting ne sont pas identiques aux champs Paramètres de la base de données de référentiel (de bibliothèque). Pour accéder aux descriptions des autres champs, consultez l'étape 20.

    Option activée : copie les paramètres de la base de données de référentiel dans cette boîte de dialogue. Cette option peut vous faire gagner du temps si vous utilisez le même serveur de base de données pour les deux bases de données CA Process Automation.

    Option désactivée : ne copiez pas les paramètres de la base de données de référentiel dans cette boîte de dialogue. Cette option est appropriée si vous utilisez deux types de base de données distincts pour les données de reporting et les enregistrements d'exécution.

    Base de données de reporting

Définit le nom de la base de données de reporting qui stocke tous les rapports générés. Entrez un nom unique.

25. Cliquez sur Suivant.
26. Sélectionnez les fichiers JAR supplémentaires (il s'agit généralement des pilotes JDBC) que vous voulez inclure dans l'installation.

    Par défaut, les pilotes JDBC chargés dans l'installation de logiciels tiers sont affichés et désactivés. Vous pouvez utiliser le bouton Ajouter des fichiers pour ajouter d'autres fichiers JAR.

    Sélectionnez chaque fichier JAR que vous voulez déployer. Vérifiez que vous avez sélectionné tous les pilotes que vous voulez déployer pour l'utilisation d'opérateurs JDBC dans des agents et des orchestrateurs CA Process Automation. Utilisez le bouton Ajouter des fichiers pour ajouter plus de pilotes.

    Il n'est pas nécessaire de prévoir les besoins des concepteurs au niveau des pilotes JDBC, étant donné que les administrateurs de domaine peuvent déployer des pilotes JDBC lorsqu'ils le souhaitent.

    Remarque : Pour plus d'informations sur l'ajout et la gestion des ressources des orchestrateurs et des agents, y compris les fichiers JAR JDBC, consultez le Manuel de l'administrateur de contenu.

    Lorsque vous avez sélectionné tous les fichiers JAR de votre choix, cliquez sur Suivant.
27. Surveillez la progression de l'installation. Le programme d'installation copie et signe tous les composants CA Process Automation. L'installation peut prendre quelques minutes.
28. Pour quitter le programme d'installation, cliquez sur Terminer .

    L'installation de l'orchestrateur de domaine est terminée.

    La première fois que vous démarrez CA Process Automation après une mise à niveau ou une installation, vous pouvez observer un délai supplémentaire dû à l'ajustement du schéma de base de données. Pour un manuel de référence, cela peut prendre 1 heure par Go de données ; toutefois, cela variera selon le fournisseur du SGBD, des spécifications de l'ordinateur et du volume de données. Démarrez l'orchestrateur (page 139). Avant de poursuivre l'installation ou la mise à niveau d'autres composants système, vérifiez que l'opération de cet orchestrateur initial s'est correctement déroulée.

Installation autonome de l'orchestrateur de domaine

CA Process Automation permet d'installer l'orchestrateur de domaine silencieusement ou de manière autonome, à l'aide d'un fichier de réponse. Le fichier de réponse contient divers paramètres prédéfinis utilisés au cours du processus d'installation. Une fois que vous créez un fichier de réponse, vous pouvez modifier et exécuter le fichier de script d'installation pour commencer l'installation.

Un exemple de fichier de réponse est fourni dans le dossier racine du DVD 1. Il est recommandé d'utiliser une copie de ce fichier comme base pour votre fichier de réponse.

Création d'un fichier de réponse

Pour effectuer une installation silencieuse de CA Process Automation, vous devez créer en premier lieu un fichier de réponse.

Prenez en compte les remarques suivantes relatives au fichier de réponse :

- Ne changez pas les noms de variables car l'installation utilise les noms de variables existants.
- Utilisez des barres obliques (/) comme séparateurs de répertoires pour spécifier des emplacements de dossier.
- Utilisez le signe dièse (#) pour placer en commentaire les variables que vous ne voulez pas utiliser.
- Consultez le journal d'installation suivant pour passer en revue les erreurs :

  ```
  ${répertoire_installation}/server/c2o/installation.log
  ```

Procédez comme suit :

1. Insérez le DVD 1 du support d'installation CA Process Automation dans un lecteur ou accédez à l'emplacement dans lequel les fichiers d'installation ont été copiés précédemment à partir du support d'installation.
2. Ouvrez le dossier DVD1.

3. Ouvrez le fichier suivant.

   `response.varfile`

4. Fournissez les valeurs de paramètre appropriées.

   Le fichier varfile inclut des descriptions de paramètre. Par exemple, pour permettre à CA EEM d'utiliser le protocole NTLM pour authentifier les utilisateurs CA Process Automation, utilisez le paramètre suivant :

   `enableNTLM=true`

   Les paramètres requis sont disponibles à cet emplacement.

5. Enregistrez le fichier varfile dans un emplacement qui contient le fichier de script d'installation silencieuse.

   Le fichier de réponse est créé.

Paramètres requis dans le fichier response.varfile

Comme indiqué précédemment, un exemple de fichier de réponse est fourni dans le dossier racine du DVD1. Les paramètres requis pour effectuer une installation autonome de CA Process Automation comprennent les éléments de la liste suivante. Les paramètres non inclus dans cette liste sont facultatifs.

License

thirdPartyLicenseAccepted

licenseAccepted

Emplacement d'installation

sys.installationDir

Emplacement Java

javaHome

Emplacement DVD2

domainInstallerDir

Mode de communication

isSecure (true/false)

Détails de base de données

- databaseType
- dbUserName
- databaseServer
- databasePortNumber
- libDb
- driver
- runtimeDbType
- runtimeDbUserName
- runtimeDbServer
- runtimeDbPort
- runtimeDb
- runtimeDriver
- reportingDbType
- reportingDbUserName
- reportingDbServer
- reportingDbPort

- reportingDb
- reportingDriver

Détails de CA EEM

- registerApplication (défini sur true pour une mise à niveau)
- upgradeApplication (défini sur true pour une mise à niveau)
- eiamServer
- eiamAppName
- eiamAdminUsrName
- eiamSDKLevel

Nouveaux paramètres pour CA Process Automation 4.2 :

nodeCommsV2Port

Port utilisé pour les communications simplifiées de l'orchestrateur de domaine

eiamSDKLevel

Entrée pour le niveau du kit de développement logiciel de CA EEM

#hasOracleConnectionString

Spécifie si une URL de connexion est requise. Cela concerne uniquement Oracle.

#dbOracleConnectionString

URL de connexion JDBC

Exemple :

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST
=<nom hôte BdD>) (PORT=<numéro port>))
(CONNECT_DATA=(SERVICE_NAME=<libDb>))).
```

Remarque : Les deux dernières entrées apparaissent à trois reprises, deux fois pour chaque base de données. Ces paramètres s'appliquent uniquement si vous sélectionnez Oracle comme base de données et que vous utilisez une chaîne de connexion.

Exécution ou modification du fichier de script d'installation silencieuse

Après avoir créé le fichier de réponse, utilisez l'une des options suivantes pour commencer l'installation silencieuse :

- Exécutez le fichier de script d'installation silencieuse et indiquez les paramètres associés dans l'invite de commande. Il s'agit de l'option recommandée quand vous installez un seul orchestrateur.
- Modifiez les paramètres du fichier de script d'installation, puis exécutez le script. Il s'agit de l'option recommandée quand vous installez plusieurs orchestrateurs.

Utilisez le fichier de script d'installation adapté à votre environnement d'exploitation :

Remarque : Sous UNIX, si vous appelez le fichier de script d'installation à l'aide du signe du dollar ($) dans un paramètre, faites-le précéder d'une barre oblique inversée (\). Par exemple, si le mot de passe de base de données est abc$123, utilisez la barre oblique inversée (\) comme préfixe : abc\$123.

Windows

Syntaxe

```
Silent_Install_windows.bat [Parameter1] [Parameter2]
[Parameter3]...
```

Utilisation :

```
Silent_Install_windows.bat -VcertPassword=a
-VeiamCertPass=eiamadmin -VeiamPassword=eiamadmin
-VdbPassword=sa -VreportingDbPassword=sa -VruntimeDbPassword=sa
-VeiamAdminPass=eiamadmin
```

UNIX

Syntaxe

```
Silent_Install_unix.sh [Parameter1] [Parameter2] [Parameter3]...
```

Utilisation :

```
Silent_Install_unix.sh -VcertPassword=a -VeiamCertPass=eiamadmin
-VeiamPassword=eiamadmin -VdbPassword=sa
-VreportingDbPassword=sa -VruntimeDbPassword=sa
-VeiamAdminPass=eiamadmin
```

Les scripts d'installation incluent les paramètres suivants :

-VcertPassword=*value*

Définit le mot de passe qui contrôle l'accès aux clés de chiffrement des mots de passe.

-VeiamCertPass

Définit le mot de passe de certificat CA EEM (par exemple, pamadmin).

-VeiamPassword

Spécifie le mot de passe de la base de données utilisée pour des objets d'automatisation (par exemple, pamadmin).

Remarque : VeiamPassword est le mot de passe de domaine Windows.

-VdbPassword

Définit le mot de passe de la base de données utilisée pour l'automatisation (par exemple, objectsroot).

-VreportingDbPassword

Définit le mot de passe de la base de données de reporting (par exemple, root).

-VruntimeDbPassword

Définit le mot de passe de la base de données qui est utilisée au moment de l'exécution (par exemple, root).

-VeiamAdminPass

Définit le mot de passe de l'administrateur CA EEM, où la valeur de nom d'utilisateur est EiamAdmin (par exemple, eiamadmin).

Important : Les paramètres de mot de passe transférés dans la ligne de commande ou stockés dans le fichier de script d'installation ne sont *pas* chiffrés.

Une fois l'installation terminée, vous pouvez démarrer l'orchestrateur. Consultez le fichier installation.log en cas d'erreur à l'issue de l'exécution du script (install_dir\server\c2o).

Remarques concernant la mise à niveau (installation silencieuse)

Avant d'effectuer une mise à niveau autonome vers CA Process Automation 4.2, recherchez le fichier response.varfile dans l'installation actuelle de CA Process Automation.

Vous pourrez trouver ce fichier à l'emplacement suivant :

```
<répertoire_installation>\server\c2o\.install4j\response.varfile
```

Vous devez connaître les valeurs des paramètres requis (page 120) pour effectuer la mise à niveau vers CA Process Automation 4.2. Une fois que vous avez obtenu ces valeurs, lancez la mise à niveau autonome à l'aide de la même commande que celle d'une nouvelle installation (page 121).

Remarque : Les pilotes jTDS sont requis dans CA Process Automation 4.2. jtds-1.3.1.jar est inclus dans le dossier de pilotes du dossier DVD1. Tout paramètre du fichier response.varfile d'une installation précédente qui inclut une référence à un fichier JAR SQL doit désormais être remplacé par une valeur jTDS dans response.varfile de CA Process Automation 4.2.

Par exemple, un fichier response.varfile de CA Process Automation 3.1 peut inclure le paramètre suivant :

```
runtimeDriver=C:/Users/Administrator/Desktop/2013_11_11/DVD1/drivers/sqljdbc.jar
```

Dans CA Process Automation 4.2, ce paramètre devient :

```
runtimeDriver=C:/Users/Administrator/Desktop/2013_11_11/DVD1/drivers/jtds-1.3.1.jar
```

Tâches de post-installation liées à l'orchestrateur de domaine

Effectuez les tâches de post-installation applicables.

- Si vous avez réinstallé (et non mis à niveau) l'orchestrateur de domaine afin de pouvoir définir des communications sécurisées à l'aide de HTTPS, reportez-vous à la section Activation des communications sécurisées pour le serveur CA Process Automation existant (page 171).
- Si vous venez d'effectuer la toute première installation de CA Process Automation, réalisez les opérations suivantes :
  - Avant de configurer les ports, vérifiez les conditions requises pour la planification des ports (page 93).
  - Activation de la communication bidirectionnelle au niveau du pare-feu (page 129)
- Pour utiliser les opérateurs Bases de données pour la connexion à des bases de données à l'aide d'un SGBDR différent de celui utilisé par CA Process Automation, installez les pilotes correspondants à ces opérateurs (page 130).

  Pour utiliser l'authentification Windows (sécurité intégrée) avec JDBC pour un serveur MS SQL Server, installez les pilotes correspondants aux opérateurs de base de données (page 130).
- Si vous avez installé l'orchestrateur de domaine sur un serveur équipé du système d'exploitation HP-UX, effectuez les étapes de configuration supplémentaires requises sous HP-UX.
- Si vous avez installé CA EEM avec Microsoft Active Directory comme répertoire externe, CA EEM peut authentifier les utilisateurs à l'aide du protocole NTLM. Si vous n'avez pas choisi d'activer l'authentification directe NTLM pendant l'installation, vous pouvez l'activer manuellement maintenant. Reportez-vous à la section Activation de l'authentification directe NTLM après l'installation (page 131).
- Les tâches de déploiement des pilotes requis pour les opérateurs de base de données requièrent le redémarrage de l'orchestrateur de domaine.
  - Voir Arrêt de l'orchestrateur (page 138)
  - Voir Démarrage de l'orchestrateur (page 139)
- Avant de configurer le premier administrateur dans CA EEM, vous pouvez accéder à CA Process Automation et vous connecter en tant qu'administrateur par défaut.

  Voir Accès à CA Process Automation et connexion en tant qu'administrateur par défaut (page 126).

Accès à CA Process Automation et connexion en tant qu'administrateur par défaut

Beaucoup de rubriques de ce manuel assument que vous avez accès à l'interface utilisateur de CA Process Automation. Les tâches telles que le déploiement des pilotes, l'installation des orchestrateurs et l'ajout de noeuds se lancent à partir de l'onglet Configuration de CA Process Automation. Habituellement, les administrateurs se connectent à CA Process Automation avec leurs propres informations d'identification pour effectuer ces tâches.

Remarque : Pour plus d'informations sur la création de votre compte d'utilisateur, reportez-vous au *Manuel de l'administrateur de contenus*.

Pour que CA Process Automation soit accessible, les conditions suivantes doivent être remplies :

- CA EEM est en cours d'exécution.
- L'équilibreur de charge, si utilisé, est en cours d'exécution.
- Le service de l'orchestrateur de domaine démarre. Pour plus d'informations, reportez-vous à la section Démarrage de l'orchestrateur (page 139).

Si vous devez effectuer des tâches requérant un accès à CA Process Automation et qu'un compte d'utilisateur CA Process Automation ne vous a pas encore été octroyé, vous pouvez vous connecter à CA Process Automation avec les informations d'identification de l'administrateur par défaut.

Important : Les informations d'identification de l'administrateur par défaut ne sont pas disponibles si CA EEM a été configuré pour utiliser Microsoft Active Directory comme référentiel d'utilisateurs. Les informations d'identification par défaut de chaque rôle utilisateur sont disponibles uniquement si vous avez configuré CA EEM pour utiliser le référentiel d'utilisateurs local pour la création et le stockage des comptes d'utilisateurs.

Procédez comme suit :

1. Accédez à l'URL CA Process Automation appropriée. Dans l'exemple suivant, *serveur* correspond au serveur sur lequel un orchestrateur de domaine non mis en cluster a été installé. Si l'orchestrateur de domaine a été mis en cluster, *serveur* correspond au serveur équipé de l'équilibreur de charge.

   - Pour une communication sécurisée, utilisez la syntaxe suivante :

     `https://serveur:port/itpam`

     Exemples :

     `https://domainOrchestrator_host:8443/itpam`

     `https://loadBalancer_host:443/itpam`

   - Pour une communication de base, utilisez la syntaxe suivante :

     `http://serveur:port/itpam`

     Exemples :

     `http://domainOrchestrator_host:8080/itpam`

     `http://loadBalancer_host:80/itpam`

   La page de connexion à CA Process Automation s'ouvre.

   Remarque : Si l'authentification NTLM est activée et que vos informations d'identification de domaine correspondent aux informations d'identification d'un compte d'utilisateur CA EEM, l'onglet Accueil s'affiche. Pour que l'authentification NTLM soit prise en charge dans Mozilla Firefox, vous devez configurer les paramètres su navigateur. Pour plus d'informations, reportez-vous à la section Prise en charge de Mozilla.

2. Dans le champ Username, entrez **pamadmin**.
3. Dans le champ Password, entrez **pamadmin**.
4. Cliquez sur Connexion.

   CA Process Automation ouvre. L'onglet Accueil s'affiche.

5. Dans la liste déroulante Aide, cliquez sur Bibliothèque. Vérifiez que vous pouvez ouvrir la bibliothèque à partir du support clientèle de CA Technologies.
6. Si la bibliothèque ne s'ouvre pas en raison de l'absence d'accès à Internet dans l'environnement dans lequel les utilisateurs CA Process Automation travaillent :

   a. Déplacez-vous vers un emplacement de la société disposant d'un accès à Internet.

   b. Accédez à l'URL de la bibliothèque de CA Process Automation version 04.20.00. https://support.ca.com/cadocs/0/CA%20Process%20Automation%2004%202%2000-ENU/Bookshelf.html

   c. Cliquez sur le lien Télécharger la bibliothèque.

   d. Déplacez la bibliothèque de l'emplacement de téléchargement vers :

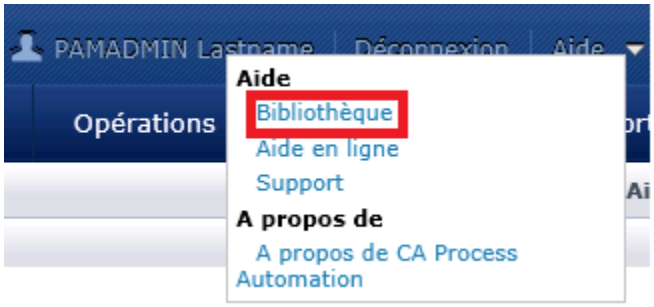
Mise à disposition de la bibliothèque pour les utilisateurs sans accès à Internet

Les utilisateurs disposant d'un accès à Internet peuvent ouvrir la bibliothèque CA Process Automation de documentation à partir du lien Bibliothèque dans CA Process Automation. Ce lien permet d'accéder à la bibliothèque de CA Process Automation 4.2 publiée sur le support clientèle de CA Technologies.

Les utilisateurs sans accès à Internet ont besoin d'aide pour disposer de la bibliothèque CA Process Automation. Pour activez le lien Bibliothèque, téléchargez la bibliothèque et déplacez-la vers un emplacement qui permettra de sélectionner la copie du serveur local.

Procédez comme suit :

1. Accédez à CA Process Automation et connectez-vous en tant qu'administrateur par défaut (page 126).
2. Dans la liste déroulante Aide, cliquez sur Bibliothèque. Vérifiez que vous pouvez ouvrir la bibliothèque à partir du support clientèle de CA Technologies.



3. Si la bibliothèque ne s'ouvre pas en raison de l'absence d'accès à Internet dans l'environnement dans lequel les utilisateurs CA Process Automation travaillent :
   a. Déplacez-vous vers un emplacement de la société disposant d'un accès à Internet.
   b. Accédez à l'URL de la bibliothèque de CA Process Automation version 04.20.00. https://support.ca.com/cadocs/0/CA%20Process%20Automation%2004%202%2000-ENU/Bookshelf.html
   c. Cliquez sur le lien Télécharger la bibliothèque.
   d. Déplacez la bibliothèque de l'emplacement de téléchargement vers :

      répertoire_installation\server\c2o\.c2orepository\bookshelf
4. Dans la liste déroulante Aide, cliquez sur Bibliothèque. Vérifiez que la bibliothèque s'ouvre.

Activation de la communication bidirectionnelle au niveau du pare-feu

Vous pouvez accéder aux composants CA Process Automation via des clients Web. Pour plus d'informations sur les ports utilisés par chaque composant dans un système CA Process Automation, consultez la rubrique Ports utilisés par CA Process Automation (page 227).

Vous devez autoriser la communication bidirectionnelle au niveau des pare-feu. Ce type de communication est requis entre les paires de composant suivantes :

- L'orchestrateur de domaine et le serveur de base de données utilisé pour la base de données de bibliothèque.
- L'orchestrateur de domaine et le serveur de base de données qu'il utilise pour sa base de données de reporting.
- L'orchestrateur de domaine et le serveur de base de données qu'il utilise pour sa base de données d'exécution.
- L'orchestrateur de domaine et CA EEM.
- Chaque orchestrateur et le serveur de base de données utilisé pour la base de données de bibliothèque.
- Chaque orchestrateur et le serveur de base de données qu'il utilise pour sa base de données de reporting.
- Chaque orchestrateur et le serveur de base de données qu'il utilise pour sa base de données de d'exécution.

Si vous utilisez des pare-feu locaux sur des ordinateurs hôtes d'orchestrateur ou d'agent, assurez-vous que les fichiers exécutables de CA Process Automation puissent écouter et se connecter de façon bi-directionnelle via le pare-feu de chaque hôte. Certains programmes de pare-feu hôte (comme le pare-feu de Windows) autorisent des exceptions pour des fichiers exécutables.

Installation des pilotes pour les opérateurs de base de données

Les concepteurs CA Process Automation peuvent utiliser des opérateurs de la catégorie Base de Données (qui remplace le module JDBC) pour se connecter aux divers systèmes de gestion de bases de données relationnelles (RDBMS). Lorsque la connexion est établie à une base de données MySQL, Oracle ou Microsoft SQL Server, les pilotes appropriés sont automatiquement mis à disposition. (La disponibilité des trois pilotes dépend de la sélection que vous avez effectuée pendant l'installation de l'orchestrateur de domaine.) Lorsque la connexion est établie à une base de données provenant d'un fournisseur différent, vous pouvez déployer le pilote JDBC pour les opérateurs de cette base de données à partir de l'onglet Configuration de CA Process Automation. Par exemple, si un concepteur veut utiliser les opérateurs de base de données pour Sybase, l'administrateur doit déployer les pilotes JDBC pour Sybase. L'administrateur peut déployer les pilotes JDBC sur des orchestrateurs ou sur des hôtes équipés d'agents CA Process Automation.

Remarque : Pour connaître les procédures à suivre, reportez-vous à la section Déploiement des pilotes JDBC pour les opérateurs de base de données dans le chapitre Gestion des ressources d'utilisateur du *Manuel de l'administrateur de contenu.*

Activation de l'authentification directe NTLM après l'installation

L'authentification directe NTLM permet à CA EEM d'authentifier des utilisateurs à l'aide du protocole NTLM. Il s'agit d'une alternative à l'utilisation des informations d'identification que les utilisateurs entrent dans la boîte de dialogue de connexion basée sur le formulaire. Avec l'authentification directe NTLM, la boîte de dialogue de connexion est omise.

La procédure suivante ne s'applique *pas* si vous avez déjà activé l'authentification directe NTLM, par exemple :

- Vous avez sélectionné l'option Activer l'authentification directe NTLM lors de l'installation interactive de CA Process Automation.
- Vous avez spécifié enableNTLM=true dans le fichier response.varfile utilisé pour installer CA Process Automation silencieusement.

Vous pouvez activer l'authentification directe NTLM en ajoutant manuellement ntlm.enabled=true au fichier OasisConfig.properties. Procédez comme suit uniquement lorsque vous voulez activer cette fonctionnalité, mais ne l'avez pas fait lors de l'installation.

Procédez comme suit :

1. Connectez-vous en tant qu'administrateur au serveur sur lequel l'orchestrateur de domaine est installé.
2. Accédez au dossier suivant, où répertoire_installation fait référence au chemin d'accès où l'orchestrateur de domaine est installé :

   répertoire_installation`/server/c2o/.config`
3. Ouvrez le fichier OasisConfig.properties dans un éditeur.
4. Utilisez la fonction Rechercher pour localiser la propriété suivante : ntlm.enabled=
5. Modifiez la valeur de la propriété sur True :

   ```
   ntlm.enabled=true
   ```
6. Enregistrez le fichier et fermez-le.
7. Redémarrez le service de l'orchestrateur.
   a. Arrêtez l'orchestrateur (page 138).
   b. Démarrez l'orchestrateur (page 139).
8. Répétez ce processus pour chaque orchestrateur.

Interaction avec la configuration du bureau

Les orchestrateurs et les agents sont normalement exécutés en tant que services de console et n'ont pas besoin d'interagir avec le bureau. Si un orchestrateur ou un agent doit interagir avec le bureau de Windows, le service d'orchestrateur ou d'agent doit démarrer en utilisant le même compte d'utilisateur que la connexion utilisateur actuelle ou au moyen du compte du système local, avec l'option Autoriser le service à interagir avec le Bureau cochée. Cette option est cochée par défaut lorsqu'un orchestrateur ou un agent est installé. Vous pouvez aussi configurer ce service au moyen de la console de services des outils administratifs de Windows. La case à cocher accordant ce droit se trouve sous l'onglet Log On (Ouverture de session) de la fenêtre Propriétés pour le service.

Configuration de CA EEM pour permettre aux utilisateurs référencés de se connecter avec une adresse électronique

Lorsque vous installez CA Process Automation, vous pouvez configurer des utilisateurs globaux ou des groupes globaux dans la section Configuration du serveur EEM à l'aide de l'option Référencer à partir d'un annuaire LDAP externe. Vous pouvez ensuite sélectionner Plusieurs domaines Microsoft Active Directory et spécifier les domaines Active Directory dans lesquels les utilisateurs CA Process Automation potentiels sont définis. Au cours de l'installation de CA Process Automation, vous identifiez le domaine Active Directory par défaut. Les utilisateurs appartenant au domaine Active Directory par défaut peuvent se connecter à CA Process Automation avec leur nom d'utilisateur et leur mot de passe. Les utilisateurs appartenant à d'autres domaines Active Directory doivent entrer leur nom principal et leur mot de passe pour se connecter. Le format standard pour un nom principal est *domaine**nom_utilisateur*.

Vous pouvez configurer CA EEM pour authentifier les utilisateurs Active Directory avec leur adresse électronique *nom_utilisateur@domaine*. Vous configurez CA EEM de façon à rechercher l'utilisateur à l'aide de la propriété userPrincipalName.

Procédez comme suit :

1. Connectez-vous à CA EEM en tant qu'administrateur CA EEM et sélectionnez le nom de l'application que vous configurez pendant l'installation de CA Process Automation.
2. Sélectionnez l'onglet Configurer.
3. Dans la palette Référentiel d'utilisateurs, sélectionnez Mappage d'attributs LDAP.

4. Créez un mappage d'attributs à partir du mappage d'attributs existant, en remplaçant le filtre d'authentification d'utilisateur samaccountName par userPrinciaplName.
   a. Dans la liste déroulante Nom du mappage, sélectionnez Active Directory.
   b. Dans le panneau Recherche d'utilisateur, le Filtre de recherche d'utilisateurs est similaire à l'exemple suivant :

      ```
      (&(objectClass=user)(!(objectClass=computer)))
      ```

   c. Modifiez le champ Filtre d'authentification de l'utilisateur en remplaçant userPrincipalName par samaccountName. Résultats de l'exemple :

      ```
      (&(ObjectClass=user)(!(objectClass=computer)(userPrincipalName= ...
      ```

   d. {UserName} est défini comme suit :

      ```
      ))
      ```

5. Enregistrez le mappage d'attributs. Par exemple, saisissez le nom **madAuthMail** dans le champ Nom du Mappage, puis cliquez sur Enregistrer.
6. Les données du mappage d'attributs d'utilisateur ressemblent aux données suivantes :

   Nom d'utilisateur : sAMAccountName

   Prénom : givenName

   Nom : sn

   Nom d'affichage : displayName
7. Dans la section Général de la page Configuration de l'annuaire LDAP, saisissez le nom du mappage d'attributs que vous avez créé à l'étape 5. Vérifiez que vos entrées s'apparentent au texte suivant :

   Nom : *domain*

   Mappage d'attributs : madAuthMail

   Domaine : *domain*

   Noms d'hôtes sélectionnés : *hostname:*389

   Protocole : LDAP

   DN de base : ou=*mylocation*,dc=*mycompany*,dc=com

   Nom unique de l'utilisateur :
   cn=*userid*,ou=Users,ou=*mylocation*,dc=*mycompany*,dc=com

   Mot de passe de l'utilisateur : *passwordForUserid*

Conditions préalables à la synchronisation horaire

Il est recommandé de synchroniser l'heure de l'orchestrateur de domaine avec celle d'un serveur de synchronisation externe standard. Cela prépare l'orchestrateur de domaine en vue de l'ajout d'un noeud de cluster. Tous les noeuds de cluster d'un orchestrateur doivent marquer le même temps horloge, dans l'idéal synchronisé avec un serveur de synchronisation externe standard. L'équilibreur de charge ne gère pas la synchronisation de l'heure.

Informations complémentaires :

Synchronisation horaire d'un noeud de cluster (page 195)

Procédure d'installation des patchs et des connecteurs avec CA Process Automation 4.2

Cette section décrit le processus d'installation des connecteurs CA Process Automation avec JBoss 5.1 sur un hôte.

Les administrateurs peuvent installer les connecteurs CA Process Automation pour permettre les interactions avec d'autres produits (produits CA et produits tiers) pour automatiser les scénarios d'utilisation métier. Chaque connecteur fonctionne comme un module contenant un ensemble d'opérateurs. Les opérateurs interagissent avec les API d'autres produits et sont utilisés pour créer des flux CA Process Automation.

Pour cela, assurez-vous d'installer CA Process Automation sur l'hôte, car le fichier exécutable du connecteur CA Process Automation s'y trouve.

Important : Pour installer un patch et un connecteur CA Process Automation, arrêtez tous les noeuds de l'orchestrateur et installez le patch et le connecteur CA Process Automation sur tous les noeuds (domaine et non domaine).

Procédez comme suit :

1. Exécutez le fichier exécutable du connecteur CA Process Automation.

   La page Bienvenue dans... s'affiche.

2. Acceptez le contrat de licence et cliquez sur Suivant.
3. Dans la page Sélectionner le répertoire d'installation de CA Process Automation, spécifiez l'emplacement du *répertoire d'installation*.
4. Dans la page Sélectionner les connecteurs à installer/mettre à jour, sélectionnez les connecteurs à installer, puis cliquez sur Suivant.

   Le connecteur CA Process Automation est installé.

5. Pour vérifier l'installation du connecteur CA Process Automation, accédez à CA Process Automation et connectez-vous. Cliquez sur l'onglet Concepteur et cliquez sur Nouveau processus.

   Le connecteur CA Process Automation installé et ses opérateurs sont répertoriés dans la vue Opérateurs.

Modification de la configuration du serveur de base de données Oracle pour utiliser RAC Oracle

Vous pouvez continuer à utiliser le serveur de base de données Oracle installé pour CA Process Automation et configuré lors de l'installation de CA Process Automation. Si ce serveur Oracle unique est inclus dans un déploiement RAC Oracle mis en cluster, vous pouvez également configurer RAC Oracle comme serveur de base de données pour une tâche de post-installation.

Procédez comme suit :

1. Vérifiez que CA Process Automation utilise le serveur de base de données Oracle unique configuré spécifié lors de l'installation de la base de données de la bibliothèque, la base de données d'exécution et la base de données de reporting.
2. Arrêtez le service CA Process Automation comme indiqué dans la section Arrêt de l'orchestrateur (page 138).
3. Ouvrez le fichier OasisConfig.properties.

   répertoire_installation\server\c2o\.config\OasisConfig.properties
4. Modifiez les entrées suivantes dans la base de données de bibliothèque :

   ```
   oasis.database.connectionurl=jdbc:oracle:thin:@//oracle-server:1521/
   oasis.database.lib.dbname=ServiceName
   oasis.database.queues.dbname=ServiceName
   oasis.database.dbhostname=Oracle-RAC
   ```
5. Modifiez les entrées suivantes dans la base de données d'exécution :

   ```
   oasis.runtime.database.connectionurl=jdbc:oracle:thin:@//oracle-server:1521/
   oasis.runtime.database.dbname=ServiceName
   oasis.runtime.database.dbhostname=Oracle-RAC
   ```
6. Modifiez les entrées suivantes dans la base de données de reporting :

   ```
   oasis.reporting.database.connectionurl=jdbc:oracle:thin:@//oracle-server:1521/
   oasis.reporting.database.dbname=ServiceName
   oasis.reporting.database.dbhostname=Oracle-RAC
   ```
7. Enregistrez le fichier OasisConfig.properties.
8. Démarrez l'orchestrateur (page 139).

Remarque : Les notations suivantes sont également valides pour les instructions sur l'URL de connexion :

Notation TNS

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=ora
cle-server)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=ServiceName)
))
```

Notation RAC TNS

```
jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=OFF)(FAILOVER=ON)(
ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=oracle-server)(PORT=1
521))(ADDRESS=(PROTOCOL=TCP)(HOST=oracle-server)(PORT=1521)))(C
ONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=ServiceName)))
```

Autre notation (sans barre oblique ; instruction terminée par deux-points)

```
jdbc:oracle:thin:@oracle-server:1521:
```

Arrêt de l'orchestrateur

Seuls les administrateurs disposant d'informations d'identification d'administrateur sur le serveur sur lequel l'orchestrateur est installé peuvent arrêter celui-ci.

Important : Si un orchestrateur n'est pas arrêté de façon appropriée, le dossier temporaire suivant peut accumuler plusieurs gigaoctets de fichiers. Si cela se produit, vous pouvez supprimer le dossier tmp en toute sécurité :

répertoire_installation/server/c2o/tmp

Procédez comme suit :

1. A l'aide des informations d'identification de l'administrateur, connectez-vous à l'hôte sur lequel l'orchestrateur cible est installé.
2. Si vous vous êtes connecté à un hôte Windows, vous pouvez arrêter le service de l'orchestrateur à partir du menu Démarrer, Services Windows, ou de la ligne de commande. Effectuez l'une des opérations suivantes :
   - Dans le menu Démarrer, sélectionnez Programmes, CA, CA Process Automation 4.0, puis Arrêter le service de l'orchestrateur.
   - Dans Panneau de configuration, sélectionnez Outils d'administration et Services. Sélectionnez le service suivant et cliquez sur Arrêter :

     `Orchestrateur CA Process Automation (C:/Program Files/CA/PAM/server/c2o)`
   - Ouvrez une fenêtre d'invite de commande et exécutez le script suivant :

     répertoire_installation/server/c2o/bin/stopc2osvc.bat
3. Si vous vous êtes connecté à un hôte UNIX ou Linux, procédez comme suit :
   a. Remplacez les répertoires par ${PAM_HOME}/server/c2o/. Par exemple, remplacez les répertoires comme suit :

      `/usr/local/CA/PAM/server/c2o`
   b. Exécutez le script c2osvrd.sh avec l'option stop. Exemple :

      `./c2osvrd.sh stop`

Démarrage de l'orchestrateur

Seuls les administrateurs disposant d'informations d'identification d'administrateur sur le serveur sur lequel l'orchestrateur est installé peuvent redémarrer celui-ci.

Procédez comme suit :

1. A l'aide des informations d'identification de l'administrateur, connectez-vous à l'hôte sur lequel l'orchestrateur cible est installé.
2. Si vous vous êtes connecté à un hôte Windows, vous pouvez redémarrer le service de l'orchestrateur à partir du menu Démarrer, Services Windows, ou de la ligne de commande. Effectuez l'une des tâches suivantes :
   - Dans le menu Démarrer, sélectionnez Programmes, CA, CA Process Automation, puis Démarrer le service de l'orchestrateur.
   - Dans Panneau de configuration, sélectionnez Outils d'administration et Services. Sélectionnez le service suivant et cliquez sur Démarrer :

     `Orchestrateur CA Process Automation (C:/Program Files/CA/PAM/server/c2o)`
   - Ouvrez une fenêtre d'invite de commande et exécutez le script suivant :

     répertoire_installation`/server/c2o/bin/startc2osvc.bat`
3. Si vous vous êtes connecté à un hôte UNIX ou Linux, procédez comme suit :
   a. Remplacez les répertoires par ${PAM_HOME}/server/c2o/. Par exemple, remplacez les répertoires comme suit :

      `/usr/local/CA/PAM/server/c2o`
   b. Exécutez le script c2osvrd.sh contenant l'option - start (Démarrer). C'est-à-dire, exécutez :

      `./c2osvrd.sh start`

Remarque : Après avoir démarrer le service de l'orchestrateur de domaine, démarrez CA Process Automation.

Désinstallation de l'orchestrateur de domaine

Seuls les administrateurs disposant d'informations d'identification d'administrateur sur le serveur sur lequel l'orchestrateur est installé peuvent le désinstaller.

Remarque : Arrêtez l'orchestrateur de domaine avant de le désinstaller.

Procédez comme suit :

1. A l'aide des informations d'identification de l'administrateur, connectez-vous à l'hôte sur lequel l'orchestrateur de domaine est installé.
2. Si vous vous êtes connecté aux hôtes suivants :
   a. Hôte Windows :
   Vous pouvez désinstaller l'orchestrateur de domaine à partir du menu Démarrer, Panneau de configuration. Effectuez l'une des tâches suivantes :
      - Dans le menu Démarrer, sélectionnez Programmes, CA, CA Process Automation 4.2, puis Désinstaller CA Process Automation.
      - Sélectionnez l'entrée CA Process Automation Domain à partir du menu Démarrer, Panneau de configuration, Programmes et fonctionnalités, puis cliquez sur Désinstaller.

        L'assistant de désinstallation s'affiche.

   b. Hôte UNIX ou Linux :
      a. Remplacez les répertoires par ${PAM_HOME}/standalone/. Par exemple, remplacez les répertoires comme suit :

         ```
         /usr/local/CA/PAM/server/c2o
         ```

      b. Exécutez le script ./uninstall.

         L'assistant de désinstallation s'affiche.
3. Une fois que l'orchestrateur de domaine est désinstallé, vérifiez que les modifications suivantes ont été appliquées :
   - Dans le panneau de configuration, sélectionnez Outils d'administration, Services et vérifiez que le service CA Process Automation Domain est supprimé.
   - L'entrée CA Process Automation Domain est supprimée du menu Démarrer, Panneau de configuration, Programmes et fonctionnalités.
   - Le dossier Orchestrateur de domaine est supprimé de l'emplacement d'installation.

Chapitre 6: Mise à niveau vers la version actuelle

Vous pouvez procédez à la mise à niveau vers CA Process Automation version 4.2 à partir des versions CA Process Automation suivantes :

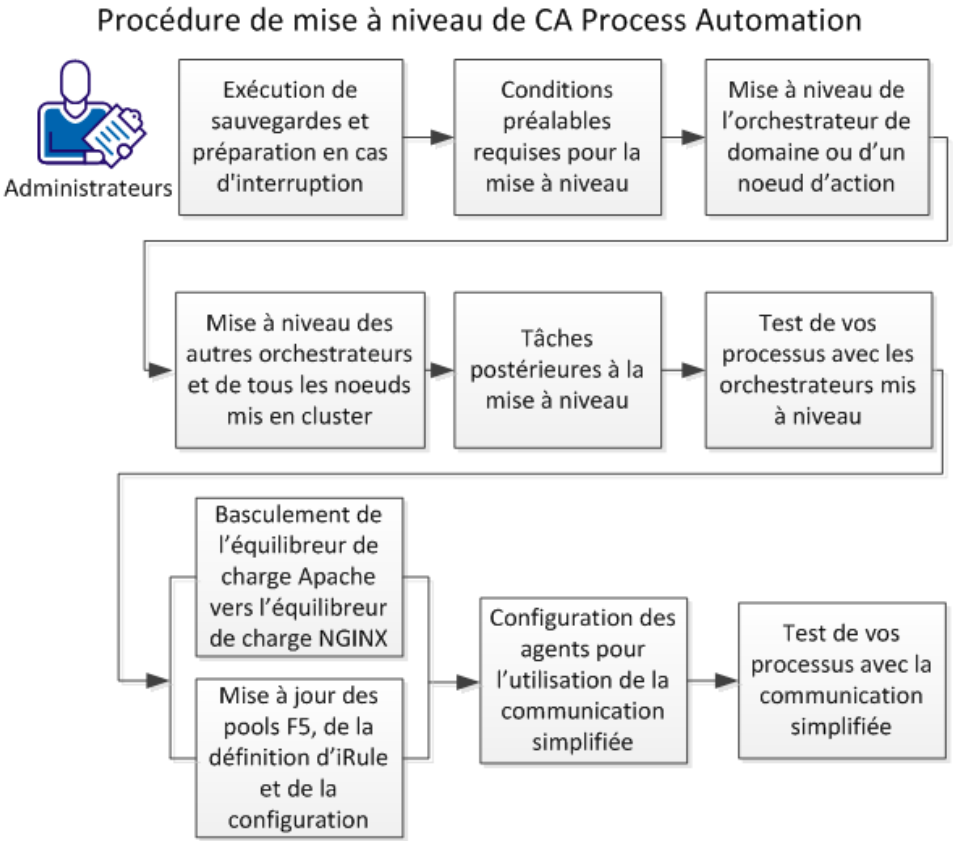
- CA Process Automation 3.1 SP01
- CA Process Automation 4.0 SP01
- CA Process Automation version 4.1
- CA Process Automation 4.1 SP01

Ce chapitre traite des sujets suivants :

Procédure de mise à niveau de CA Process Automation (page 142)
Exécution de sauvegardes et préparation en cas d'interruption (page 143)
Conditions préalables requises pour la mise à niveau (page 145)
Procédure de mise à niveau de l'orchestrateur de domaine (page 146)
Procédure de mise à niveau d'un orchestrateur de domaine non mis en cluster (page 150)
Procédure de mise à niveau d'un noeud de cluster (page 153)
Réalisation des tâches postérieures à la mise à niveau (page 156)
Test de vos processus avec les orchestrateurs mis à niveau (page 157)
Basculement de l'équilibreur de charge Apache vers l'équilibreur de charge NGINX (page 158)
Mise à jour des pools F5, de la définition d'iRule et de la configuration (page 158)
Configuration des agents pour utiliser la méthode de communication simplifiée (page 159)
Test de vos processus avec la communication simplifiée (page 160)

Procédure de mise à niveau de CA Process Automation

Vous pouvez procéder à une mise à niveau vers CA Process Automation 4.2 à partir de 3.1 SP01 et versions ultérieures à l'aide du processus illustré.


Procédure de mise à niveau de CA Process Automation
Administrateurs
Exécution de sauvegardes et préparation en cas d'interruption
Conditions préalables requises pour la mise à niveau
Mise à niveau de l'orchestrateur de domaine ou d'un noeud d'action
Mise à niveau des autres orchestrateurs et de tous les noeuds mis en cluster
Tâches postérieures à la mise à niveau
Test de vos processus avec les orchestrateurs mis à niveau
Basculement de l'équilibreur de charge Apache vers l'équilibreur de charge NGINX
Mise à jour des pools F5, de la définition d'iRule et de la configuration
Configuration des agents pour l'utilisation de la communication simplifiée
Test de vos processus avec la communication simplifiée

Important : Avant de lancer le processus décrit ici, effectuez une mise à niveau à partir d'une version antérieure à r3.1 SP01 (page 298) si nécessaire.

Procédez comme suit :

1. Exécution de sauvegardes et préparation en cas d'interruption (page 143)
2. Exécution des conditions préalables requises pour la mise à niveau (page 145)
3. Procédure de mise à niveau de l'orchestrateur de domaine (page 146)
4. Procédure de mise à niveau des autres orchestrateurs et de tous les noeuds mis en cluster
   - Procédure de mise à niveau d'un orchestrateur de domaine non mis en cluster (page 150)
   - Procédure de mise à niveau d'un noeud de cluster (page 153)
5. Réalisation des tâches postérieures à la mise à niveau (page 156)
6. Test de vos processus avec les orchestrateurs mis à niveau (page 157)
7. Le serveur d'annuaire doit être l'un des serveurs suivants :
   - Basculement de l'équilibreur de charge Apache vers l'équilibreur de charge NGINX (page 158)
   - Mise à jour des pools F5, de la définition d'iRule et de la configuration (page 158)
8. Configuration des agents pour utiliser la communication simplifiée (page 159)
9. Test de vos processus avec la communication simplifiée (page 160)

Exécution de sauvegardes et préparation en cas d'interruption

Des incidents imprévus ou incontrôlables peuvent interrompre le processus de mise à niveau ou entraîner son échec. Par mesure de précaution, il est recommandé de sauvegarder toutes les données importantes stockées dans des dossiers CA Process Automation avant de lancer la mise à niveau. Pour préparer la restauration complète, sauvegardez également le contenu CA Process Automation que vous stockez dans vos serveurs de base de données et dans CA EEM.

Procédez comme suit :

1. Vérifiez que vos serveurs de base de données peuvent accéder à au moins le double de l'espace actuellement utilisé par vos bases de données CA Process Automation existantes.
2. Pour vous préparer à une potentielle restauration, effectuez des clichés de tous les ordinateurs virtuels de l'orchestrateur ou sauvegardez le dossier suivant sur tous les orchestrateurs :

   `répertoire_installation/server/c2o`

   Il est recommandé de sauvegarder ce dossier vers un disque physique différent de celui qui héberge le dossier *répertoire_installation.*

3. Avant leur mise à niveau, sauvegardez les référentiels de données de bibliothèque, d'exécution et de reporting utilisés par chaque orchestrateur. Les référentiels de données peuvent résider sur différents serveurs de base de données ou sur le même serveur de base de données.
4. Sauvegardez l'application CA Process Automation dans votre serveur CA EEM.
   a. Connectez-vous à CA EEM, en spécifiant l'application CA Process Automation.
   b. Cliquez sur l'onglet Configurer, puis sur Serveur EEM et sur Application d'exportation.
   c. Cliquez sur Exporter et enregistrez le fichier <nom de l'application>.gz dans votre lecteur local.
5. Réalisez les préparations en cas d'interruption. La durée de mise à niveau d'un orchestrateur dépend de la taille des référentiels de données. Plus ils contiennent de données, plus la mise à niveau sera longue.
   - Si vous disposez d'autres applications qui reposent sur des services CA Process Automation, préparez-vous à cette interruption. Par exemple, si vous utilisez CA Service Catalog pour initialiser des processus CA Process Automation, vous pouvez le fermer pendant la mise à niveau CA Process Automation. De même, vous pouvez présenter une boîte de dialogue indiquant l'indisponibilité temporaire des éléments de catalogue qui reposent sur CA Process Automation, puis supprimer cette boîte de dialogue à l'issue de la mise à niveau de CA Process Automation.
   - Planifiez une fenêtre de maintenance appropriée et informez les partenaires concernés de l'intervalle de temps pendant lequel CA Process Automation devrait être indisponible.

Conditions préalables requises pour la mise à niveau

Avant de démarrer le processus de mise à niveau vers la version 04.2.00 de CA Process Automation, effectuez les tâches obligatoires suivantes :

1. Ayez à portée de main les informations d'identification de l'administrateur de CA EEM, où EiamAdmin est généralement le nom de l'administrateur de CA EEM et le mot de passe de l'administrateur de CA EEM est connu de l'administrateur de CA EEM.
2. Enregistrez le mot de passe de certificat à utiliser pour cette mise à niveau du système.

   Le mot de passe de certificat permet de contrôler l'accès aux clés utilisées pour chiffrer les mots de passe et d'autres données critiques. Spécifiez ce mot de passe pour le premier orchestrateur que vous mettez à niveau. Puis, vous devez entrer ce même mot de passe lors de l'installation d'autres noeuds de l'orchestrateur de domaine, d'autres orchestrateurs autonomes et de noeuds d'autres orchestrateurs mis en cluster pour la même version.

   Important : Vous devez utiliser le même mot de passe de certificat utilisé avec la version à partir de laquelle vous effectuez la mise à niveau.
3. Vérifiez qu'aucun processus CA Process Automation n'est actif, c'est-à-dire dont l'état est défini sur En cours d'exécution ou Bloqué.
4. Arrêtez tous les orchestrateurs, sauf l'orchestrateur de domaine. Pour les orchestrateurs mis en cluster autres que l'orchestrateur de domaine, arrêtez le service d'orchestrateur sur chaque noeud. Voir Arrêt de l'orchestrateur (page 138)
5. Arrêtez l'orchestrateur de domaine. Pour un orchestrateur de domaine mis en cluster, arrêtez le service d'orchestrateur sur chaque noeud. Voir Arrêt de l'orchestrateur (page 138)

   Remarques :

   - Les agents actifs ne parviennent pas à se connecter aux orchestrateurs arrêtés, mais pourront s'y reconnecter une fois que les orchestrateurs sont redémarrés.
   - Les processus planifiés et les opérateurs ne seront pas exécutés lors du processus de mise à niveau.

6. Si vous utilisez un équilibreur de charge Apache, copiez les modèles de configuration d'Apache mis à jour à partir de DVD1. Pour plus d'informations, reportez-vous à la section Equilibreur de charge Apache (page 261).
7. Si vous utilisez un équilibreur de charge F5, mettez à jour la définition d'iRule pour supprimer la désignation du noeud principal. Ce changement rend possible la poursuite de l'utilisation de la communication désapprouvée lors de la première phase de la mise à niveau.
   a. Supprimer : set PRIMARY "[PrimaryIP]"
   b. Supprimer : set PRIMPORT "[PrimaryPort]"
   c. Supprimez toutes les occurrences : member $PRIMARY $PRIMPORT
8. Vérifiez que la version du kit de développement Java installé sur tous les noeuds de l'orchestrateur est prise en charge. Voir Configuration requise pour le kit de développement Java (page 77)
9. Si le nom d'hôte DNS défini lors de l'installation de CA Process Automation contenait des caractères interdits (tels que des traits de soulignement), corrigez-le. Pour plus d'informations, reportez-vous à la section Résolution des caractères non valides dans le nom DNS de CA Process Automation. (page 248)
10. Vérifiez que CA EEM est en cours d'exécution.

    Remarque : Si vous avez utilisé un serveur LDAP différent de CA Embedded Entitlements Manager (CA EEM), installez CA EEM et démarrez-le. CA EEM est le seul serveur d'annuaire pris en charge par CA Process Automation 4.0 et les versions ultérieures.
11. Effectuez la mise à niveau de chaque connecteur CA Process Automation autres que les connecteurs 4.x.

Procédure de mise à niveau de l'orchestrateur de domaine

Vous pouvez procéder directement à la mise à niveau vers CA Process Automation 4.2. à partir des versions de CA Process Automation suivantes :

- CA Process Automation Service Pack 3.1sp01
- CA Process Automation Service Pack 4.0sp01
- CA Process Automation 4.1
- CA Process Automation Service Pack 4.1sp01

Procédez comme suit :

1. Connectez-vous à l'hôte sur lequel l'orchestrateur de domaine (ou un noeud de l'orchestrateur de domaine) est installé.
2. Accédez au dossier DVD1 sur le média d'installation et lancez l'assistant d'installation à partir du fichier de votre système d'exploitation :
   - **Windows :** Domain_Installer_windows.bat
   - **Linux ou UNIX :** Domain_Installer_unix.sh

   Ces fichiers appellent le programme d'installation tiers, puis le programme d'installation de l'orchestrateur de domaine.
3. Pour parcourir les pages initiales de l'assistant, cliquez sur Suivant :
   - Langue
   - Bienvenue dans l'assistant de configuration du programme d'installation de composants tiers CA Process Automation
   - Contrat de licence - J'accepte les termes du contrat de licence.
   - Sélectionner le répertoire de destination
   - Conditions préalables à l'installation de CA Process Automation
4. Lorsque la fenêtre Installation de fichiers .jar de JDBC s'affiche,
   - cliquez sur Suivant si vous utilisez Oracle comme serveur de base de données.
   - Cliquez sur Ajouter des fichiers si vous utilisez MySQL ou SQL Server comme serveur de base de données.
     - Si vous utilisez MySQL, accédez à l'emplacement dans lequel vous avez téléchargé le fichier .jar approprié.
     - Si vous utilisez SQL Server, accédez au fichier DVD1\drivers\jtds-1.3.jar.
5. Dans la fenêtre Conditions préalables à l'installation de CA Process Automation, cliquez sur Suivant.
6. Lorsque la fenêtre Fin de l'assistant d'installation de CA Process Automation s'affiche, remplacez DVD1 par DVD2 dans le chemin d'accès au répertoire. Puis, cliquez sur Terminer.

   Le message Veuillez patienter pendant la copie du programme d'installation de CA Process Automation s'affiche. Cette opération peut prendre quelques minutes. Il peut exister un décalage entre la fermeture de cette page et l'ouverture de la page de bienvenue.
7. Lorsque la fenêtre Bienvenue dans l'assistant d'installation de CA Process Automation s'affiche, cliquez dans les pages initiales de l'assistant :
   - Langue
   - Bienvenue dans l'assistant d'installation de CA Process Automation
   - Contrat de licence - J'accepte les termes du contrat de licence.

8. Vérifiez que le répertoire de base Java pointe vers la version du kit de développement Java prise en charge par cette version.
9. Pour continuer, cliquez dans les pages :
   - Réinstaller
   - Fenêtre Configuration
10. Lorsque la fenêtre Définir le mot de passe de certificat s'affiche, saisissez le mot de passe spécifié lors de l'installation de la dernière version. Enregistrez le mot de passe à des fins de référence future, car il sera requis pour la mise à niveau de tous les autres orchestrateurs et les noeuds d'orchestrateur dans ce domaine CA Process Automation. Cliquez sur Suivant.
11. Cliquez dans Select Start Menu Folder (Sélectionner un dossier du menu Démarrer) pour utiliser votre sélection précédente.
12. Dans la page Propriétés générales, notez les changements suivants dans les valeurs par défaut du port du serveur de l'orchestrateur :

    Port du serveur

    Spécifie le port que l'orchestrateur de domaine utilise pour communiquer avec d'autres orchestrateurs et agents. Ce port est utilisé pour la communication simplifiée.

    Valeur par défaut : 80 pour les connexions de base HTTP ou 443 pour les connexions sécurisées HTTPS.

    Port de serveur désapprouvé

    Valeur du port de serveur définie pour une version précédente de CA Process Automation. Ce port est utilisé pour la communication désapprouvée.

    Valeur par défaut : 7001
13. Cliquez dans les pages suivantes et apportez les changements comme il vous convient.
    - Répertoire temporaire pour l'exécution des scripts
    - Politique d'exécution PowerShell
14. Lorsque la fenêtre Paramètres de sécurité de CA Embedded Entitlements Manager (EEM) s'affiche,
    a. sélectionnez Enregistrer l'application dans CA EEM et cliquez sur Enregistrer.
    b. Indiquez les informations d'identification pour vous connecter à CA EEM en tant qu'administrateur EiamAdmin.
    c. Acceptez la mise à niveau. Le processus d'installation détecte la version du serveur CA EEM et sélectionne le kit de développement logiciel approprié.
    d. Lorsque le message Application enregistrée s'affiche, cliquez sur OK.

15. Cliquez dans Paramètres de la base de données, car ceux-ci ont déjà été définis :
    - Base de données de référentiel
    - base de données d'exécution
    - base de données de reporting
16. Cliquez dans Fichiers JAR supplémentaires à installer si vous n'avez aucun élément à ajouter.
17. Lorsque la fenêtre Fin de l'assistant d'installation de CA Process Automation s'affiche, cliquez sur Terminer.

    Important : L'orchestrateur de domaine sera disponible pour la connexion après une période de temps significative. La mise à niveau d'autres orchestrateurs ou noeuds supplémentaires, lorsque l'orchestrateur de domaine est mis en cluster, peut démarrer uniquement après votre connexion à l'orchestrateur de domaine.
18. Démarrez le service de l'orchestrateur sur l'orchestrateur de domaine.

    Remarque : Pour obtenir des détails spécifiques au système d'exploitation, reportez-vous à la section Démarrage d'orchestrateurs (page 139).

Tâches supplémentaires de mise à niveau à l'issue de l'assistant d'installation de domaine

1. Envisagez de régler la machine virtuelle Java en mettant à jour les valeurs dans *répertoire_installation*/server/c2o/bin/c2osvcw.conf. Exemple :

   ```
   wrapper.java.additional.7=-XX:PermSize=256m
   wrapper.java.additional.8=-XX:MaxPermSize=768m
   wrapper.java.initmemory=4096
   wrapper.java.maxmemory=4096
   ```

   Les valeurs wrapper.java.initmemory et wrapper.java.maxmemory doivent être identiques. Si de la mémoire supplémentaire est requise et disponible sur le serveur, vous pouvez changer ces valeurs. Après avoir appliqué des modifications aux valeurs de configuration, redémarrez le service CA Process Automation.
2. Prévoyez de mettre à jour les valeurs par défaut pour les pools JBOSS JMS et de bases de données dans *répertoire_installation*/server/c2o/conf/standardjboss.xml. Exemple :
   - Sous <jndi-name> DefaultDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <prepared-statement-cache-size>250</prepared-statement-cach
     e-size>
     <max-pool-size>375</max-pool-size>
     ```
   - Sous <jndi-name> DDLDatasourceDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <max-pool-size>375</max-pool-size>
     ```

3. Si vous utilisez CA EEM 12.51 avec CA Process Automation mis à niveau et que vous avez configuré CA EEM pour référencer plusieurs annuaires Microsoft Active Directory ou une forêt Active Directory, recréez des utilisateurs CA Process Automation dans CA EEM.

   Remarque : Reportez-vous à la section relative à la gestion des accès pour les comptes d'utilisateurs référencés dans le *Manuel de l'administrateur de contenu*.

Informations complémentaires :

Remarques concernant la mise à niveau (installation silencieuse) (page 124)

Procédure de mise à niveau d'un orchestrateur de domaine non mis en cluster

A l'issue de la mise à niveau de l'orchestrateur de domaine en appelant un script disponible sur le média, vous pouvez mettre à niveau d'autres orchestrateurs à partir de l'interface utilisateur CA Process Automation.

Procédez comme suit :

1. Connectez-vous à l'hôte sur lequel est installé l'orchestrateur à mettre à niveau.
2. Accédez à CA Process Automation, puis connectez-vous (page 175) avec les informations d'identification de l'administrateur.
3. Cliquez sur l'onglet Configuration et sélectionnez la palette Installation.
4. Dans la section Installer un orchestrateur, cliquez sur Installer pour lancer la mise à niveau.
5. Sélectionnez une langue, puis cliquez sur OK.

   La page Bienvenue dans l'assistant de configuration du programme d'installation de composants tiers CA Process Automation s'affiche.
6. Pour accéder aux pages suivantes de l'assistant d'installation, cliquez sur Suivant :
   - Contrat de licence - Sélectionnez l'option pour accepter le contrat.
   - Répertoire d'installation par défaut
   - Conditions préalables à l'installation de CA Process Automation

7. Indiquez les fichiers JAR JDBC à installer en procédant de l'une des façons suivantes :
   - Désélectionnez la case à cocher Utiliser un domaine et cliquez sur Suivant. Cela permet d'indiquer d'utiliser les fichiers .jar JDBC configurés lors de l'installation de l'orchestrateur de domaine.
   - Procédez comme suit :
     a. Décochez la case Utiliser un domaine.
     b. Cliquez sur Ajouter des fichiers.
     c. Sélectionnez le type de serveur de base de données.
     d. Cliquez sur Parcourir et accédez au fichier JAR JDBC correspondant au type de serveur sélectionné.
     e. Cliquez sur Suivant.
8. Cliquez sur Suivant pour confirmer, puis cliquez sur Terminer pour accéder au programme d'installation de CA Process Automation.
9. Dans la page Bienvenue, cliquez sur Suivant.
10. Sélectionnez l'option pour accepter le contrat de licence et cliquez sur Suivant.
11. Lorsque la page du répertoire de base Java s'affiche, recherchez l'emplacement du kit de développement Java mis à niveau, puis cliquez sur Suivant.
12. Pour accéder aux pages suivantes de l'assistant d'installation, cliquez sur Suivant :
    - URL du domaine
    - Page d'authentification unique et de configuration de l'équilibreur de charge
    - Nom de la société
13. Saisissez un mot de passe de certificat et cliquez sur Suivant.

    Ce mot de passe de certificat est celui que l'orchestrateur de domaine utilise. Saisissez le même mot de passe de certificat saisi lors de l'installation de l'orchestrateur de domaine. Il s'agit du même mot de passe de certificat utilisé dans la version à partir de laquelle vous procédez à la mise à niveau.

14. Pour accepter la configuration précédente dans les pages de l'assistant d'installation suivantes, cliquez sur Suivant :
    - Spécifiez les préférences du dossier du menu Démarrer et cliquez sur Suivant.
    - Propriétés générales
    - Répertoire temporaire pour l'exécution des scripts
    - Politique d'exécution de PowerShell
    - Paramètres de la base de données de référentiel pour cet orchestrateur
    - Paramètres de la base de données d'exécution
    - Paramètres de la base de données de reporting
15. Cliquez sur Terminer.
16. A l'issue du traitement, démarrez le service de l'orchestrateur sur l'orchestrateur non mis en cluster mis à niveau.

    Remarque : Pour obtenir des détails spécifiques au système d'exploitation, reportez-vous à la section Démarrage d'orchestrateurs (page 139).

Tâches de mise à niveau supplémentaires

1. Envisagez de régler la machine virtuelle Java en mettant à jour les valeurs dans *répertoire_installation*/server/c2o/bin/c2osvcw.conf. Exemple :

   ```
   wrapper.java.additional.7=-XX:PermSize=256m
   wrapper.java.additional.8=-XX:MaxPermSize=768m
   wrapper.java.initmemory=4096
   wrapper.java.maxmemory=4096
   ```

   Les valeurs wrapper.java.initmemory et wrapper.java.maxmemory doivent être identiques. Si de la mémoire supplémentaire est requise et disponible sur le serveur, vous pouvez changer ces valeurs.

2. Prévoyez de mettre à jour les valeurs par défaut pour les pools JBOSS JMS et de bases de données dans *répertoire_installation*/server/c2o/conf/standardjboss.xml. Exemple :
   - Sous <jndi-name> DefaultDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <prepared-statement-cache-size>250</prepared-statement-cache-size>
     <max-pool-size>375</max-pool-size>
     ```

   - Sous <jndi-name> DDLDatasourceDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <max-pool-size>375</max-pool-size>
     ```

informations complémentaires :

Exemple : mise à niveau d'un orchestrateur non mis en cluster de 4.1 SP01 vers 4.2 sous Windows (page 292)

Procédure de mise à niveau d'un noeud de cluster

Lors de la mise à niveau d'un orchestrateur mis en cluster, procédez à la mise à niveau d'un noeud à la fois, en commençant par un noeud dans le cluster.

Procédez comme suit :

1. Connectez-vous à l'hôte sur lequel un noeud de cluster est installé.
2. Accédez à l'URL de l'orchestrateur de domaine (l'équilibreur de charge de l'orchestrateur de domaine s'il est mis en cluster).
3. Connectez-vous, cliquez sur l'onglet Configuration, puis sur la palette Installation.
4. Sous Installer le noeud de cluster pour l'orchestrateur, cliquez sur Installation pour lancer la mise à niveau.
5. La boîte de dialogue Sélection de la langue s'affiche d'abord. Cliquez sur OK.
6. Cliquez dans les pages suivantes de l'assistant :
   - Bienvenue dans l'assistant de configuration du programme d'installation de composants tiers CA Process Automation
   - Contrat de licence : sélectionnez l'option J'accepte les termes du contrat de licence.
   - Sélectionnez Répertoire de destination, par défaut : C:\Program Files\CA\PAM.
   - Conditions préalables à l'installation de CA Process Automation : appelle l'installation.
   - Fin de l'assistant d'installation de CA Process Automation et Utiliser un domaine : cliquez sur Terminer.

     Patientez jusqu'à ce que la page suivante s'affiche. Il n'existe aucun indicateur visuel du traitement précédant l'affichage de la page suivante.
   - Bienvenue dans l'assistant d'installation de CA Process Automation
   - Contrat de licence
7. Si vous avez mis à niveau votre kit de développement Java, accédez au répertoire de base Java, par exemple : C:\Program Files\Java\jdk1.7.0_45.

8. Renseignez la fenêtre Configuration :
   a. Si vous avez déjà mis à niveau un noeud dans ce cluster, sélectionnez le premier noeud d'orchestrateur mis à niveau dans la liste déroulante Orchestrateur.
   b. Saisissez node1, node2, node3, ou node4 dans le champ Noeud de travail de l'équilibreur de charge pour identifier le noeud que vous mettez à niveau.
9. S'il ne s'affiche pas, saisissez le nom de votre société.
10. Saisissez votre mot de passe de certificat.

    Important : Cette entrée doit correspondre au mot de passe de certificat saisi lors de la mise à niveau de l'orchestrateur de domaine.
11. Cliquez dans les pages suivantes, si elles s'affichent. Les paramètres utilisés par node1 sont utilisés par d'autres noeuds dans le cluster.
    - Sélectionnez un dossier du menu Démarrer.
    - Page Propriétés générales (Installer en tant que service Windows ne s'affiche pas, mais elle est prise en compte)
    - Répertoire temporaire pour l'exécution des scripts
    - PowerShell
    - Paramètres de sécurité de CA Embedded Entitlements Manager (CA EEM)
    - Paramètres de la base de données - Référentiel
    - Paramètres de la base de données - Exécution
    - Paramètres de la base de données - Reporting

    L'installation de la mise à niveau démarre.
12. Lorsque la fenêtre Fin de l'assistant d'installation de CA Process Automation s'affiche, cliquez sur Terminer.

    Le traitement se poursuit alors.
13. A l'issue du traitement, démarrez le service de l'orchestrateur sur le noeud de cluster mis à niveau.

    Remarque : Pour obtenir des détails spécifiques au système d'exploitation, reportez-vous à la section Démarrage d'orchestrateurs (page 139).

Tâches de mise à niveau supplémentaires

1. Envisagez de régler la machine virtuelle Java en mettant à jour les valeurs dans *répertoire_installation*/server/c2o/bin/c2osvcw.conf. Exemple :

   ```
   wrapper.java.additional.7=-XX:PermSize=256m
   wrapper.java.additional.8=-XX:MaxPermSize=768m
   wrapper.java.initmemory=4096
   wrapper.java.maxmemory=4096
   ```

   Les valeurs wrapper.java.initmemory et wrapper.java.maxmemory doivent être identiques. Si de la mémoire supplémentaire est requise et disponible sur le serveur, vous pouvez changer ces valeurs.

2. Prévoyez de mettre à jour les valeurs par défaut pour les pools JBOSS JMS et de bases de données dans *répertoire_installation*/server/c2o/conf/standardjboss.xml. Exemple :

   - Sous <jndi-name> DefaultDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <prepared-statement-cache-size>250</prepared-statement-cach
     e-size>
     <max-pool-size>375</max-pool-size>
     ```

   - Sous <jndi-name> DDLDatasourceDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <max-pool-size>375</max-pool-size>
     ```

Informations complémentaires :

Exemple : mise à niveau d'un noeud de l'orchestrateur de domaine de la version 3.1 SP01 vers 4.2 sous Windows (page 281)
Exemple : mise à niveau d'un autre noeud de l'orchestrateur de domaine de la version 3.1 SP01 vers 4.2 sous Windows (page 289)

Réalisation des tâches postérieures à la mise à niveau

Après avoir effectué la mise à niveau vers CA Process Automation 4.2, effectuez les tâches postérieures à la mise à niveau suivantes :

1. Reportez les modifications apportées au fichier de configuration.
   a. Accédez à l'emplacement de sauvegarde suivant :

      `install_dir/config_backup_MM_dd_yyyy_HHmm`

   b. Utilisez un outil de comparaison de fichiers pour mettre en surbrillance les différences entre les fichiers de configuration sauvegardés suivants et la version actuelle de CA Process Automation.
      `répertoire_installation/server/c2o/.config/OasisConfig.properties`
      `répertoire_installation/server/c2o/bin/c2osvcw.conf`
      `répertoire_installation/server/c2o/conf/standardjboss.xml`
      `répertoire_installation/server/c2o/conf/log4j.xml`

   c. Appliquez les changements appropriés à la version actuelle de CA Process Automation.
2. Accédez et connectez-vous à CA Process Automation. (page 175)
3. Cliquez sur l'onglet Configuration et examinez l'explorateur de configurations.
4. Vérifiez que tous les orchestrateurs s'affichent sous le noeud Orchestrateurs et que les points de contact de l'orchestrateur associé s'affichent dans la hiérarchie de domaines sous l'environnement correct. Si un orchestrateur est actif, démarrez l'orchestrateur (page 139).
5. Vérifiez que les agents sont redémarrés. Les agents utilisant la communication désapprouvée redémarrent automatiquement. Si un agent est arrêté, démarrez-le comme indiqué dans la section Démarrage d'un agent (page 186).
6. Si vous utilisez CA EEM 12.51 avec CA Process Automation mis à niveau et que vous avez configuré CA EEM pour référencer plusieurs annuaires Microsoft Active Directory ou une forêt Active Directory, rétablissez la propriété des objets.

   Remarque : Consultez la section Modification de la propriété d'un objet d'automatisation du *Manuel du concepteur de contenu.*

Test de vos processus avec les orchestrateurs mis à niveau

A l'issue de la mise à niveau, testez vos processus avec CA Process Automation mis à niveau. Tenez compte de l'approche suivante : Vérifiez que les processus s'exécutent sur chaque orchestrateur.

Procédez comme suit :

1. Démarrez un processus qui génère une tâche. Affectez-vous cette tâche. Vérifiez que l'instance de processus s'affiche dans l'onglet Accueil. Vérifiez que la tâche affectée s'affiche dans votre liste de tâches.
2. Démarrez un processus planifié ou un opérateur. Vérifiez qu'il démarre à l'heure et se termine correctement.
3. Démarrez un processus avec des opérateurs exécutés sur des points de contact d'agent ou sur des hôtes distants via des points de contact du proxy. Vérifiez que l'instance de processus se termine correctement.
4. Autorisez l'utilisation de solutions se servant de CA Process Automation comme composant intégré à exécuter. Surveillez les résultats et vérifiez qu'aucun événement inattendu ne se produit.

Basculement de l'équilibreur de charge Apache vers l'équilibreur de charge NGINX

Si vous avez utilisé un équilibreur de charge Apache pour vos orchestrateurs mis en cluster avant la mise à niveau, il est recommandé de conserver cet équilibreur de charge jusqu'à la vérification complète du fonctionnement correct de la nouvelle version. Vous devez pour cela mettre à jour la configuration d'Apache avec les nouveaux modèles fournis dans le média d'installation.

Le remplacement par NGINX suite à une mise à niveau est similaire à l'installation de NGINX dans une nouvelle version excepté pour les mises à niveau : vous devez installe NGINX sur le même serveur sur lequel l'équilibreur de charge Apache est actuellement présent. Cela vous permet d'utiliser l'URL, les noms d'hôte et les ports préalablement établis.

Pour plus d'informations sur l'installation, reportez-vous à la section Equilibreur de charge NGINX (page 35).

Les agents communiquent avec des orchestrateurs et vice versa. La version 4.2 introduit une méthode de communication simplifiée améliorée. Apache utilise la méthode de communication désapprouvée. Par défaut, les agents existants sont configurés pour utiliser la communication désapprouvée. Ce paramètre par défaut permet de basculer des équilibreurs Apache vers NGINX et de convertir les agents existants pour utiliser la communication simplifiée à un moment convenable à l'issue des tâches de mise à niveau obligatoires. NGINX prend en charge la communication simplifiée. NGINX prend également en charge la communication désapprouvée.

Mise à jour des pools F5, de la définition d'iRule et de la configuration

Pour utiliser la communication simplifiée, modifiez la configuration de F5.

Procédez comme suit :

1. Créez deux pools F5 pour chaque cluster CA Process Automation (page 55).
2. Remplacez votre iRule actuel par la définition d'iRule (page 58).
3. Configurez F5 pour utiliser la communication simplifiée HTTPS (page 61).

Configuration des agents pour utiliser la méthode de communication simplifiée

Pour basculer la communication désapprouvée vers la communication simplifiée pour les agents, vous devez réinstaller les agents existants. Cela est applicable à tous les agents une fois CA Process Automation 04.2.00 mis à niveau et après l'installation et la configuration d'un équilibreur de charge NGINX.

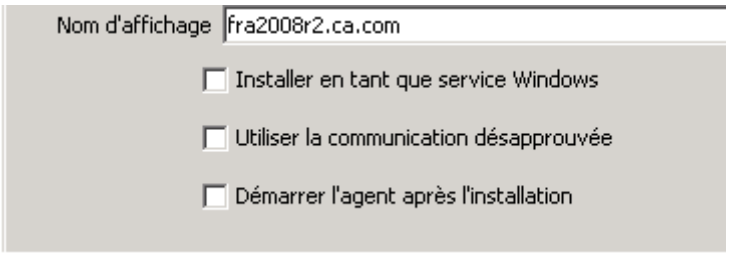
Réinstallez chaque agent comme indiqué dans la section Installation interactive d'un agent (page 176). Par défaut, la case à cocher Utiliser la communication désapprouvée est désélectionnée. Lorsque cette case à cocher est désélectionnée, l'agent est installé de sorte à utiliser la communication simplifiée.

L'agent crée des connexions de socket Web et envoie les détails de connexion à tous les noeuds de l'orchestrateur. Les orchestrateurs utilisent cette connexion persistante de socket Web pour envoyer des demandes ou des mises à jour à l'agent si nécessaire.

A propos des communications d'agent

Vous configurez les communications d'agent lorsque vous installez un agent. Par défaut, les nouveaux agents utilisent la communication simplifiée ; la case à cocher Utiliser la communication désapprouvée est désélectionnée.

Les agents mis à niveau utilisent la communication désapprouvée. Vous pouvez reconfigurer ce paramètre sans réinstaller l'agent.



Communication simplifiée

La méthode de communication simplifiée utilise des sockets Web et HTTP pour établir une connexion unilatérale persistante de l'agent vers l'orchestrateur. CA Process Automation utilise un port standard (80 ou 443) qui fournit une connexion rapide entre les composants.

Communication désapprouvée

La communication désapprouvée, qui utilise plusieurs ports, ne permet pas l'utilisation de pare-feu ou de routeur NAT, contrairement à la communication simplifiée. Les connexions initialisées par l'orchestrateur utilisées dans la communication désapprouvée ne sont pas aussi efficaces que les connexions persistantes utilisées dans la communication simplifiée.

Informations complémentaires

Ports utilisés par l'équilibreur de charge (page 231)

Test de vos processus avec la communication simplifiée

A l'issue de l'installation de l'équilibreur de charge NGINX pour chaque orchestrateur mis en cluster, testez vos processus à nouveau. Tenez compte de l'approche suivante : Vérifiez que les processus s'exécutent sur chaque orchestrateur.

Procédez comme suit :

1. Démarrez un processus qui génère une tâche. Affectez-vous cette tâche. Vérifiez que l'instance de processus s'affiche dans l'onglet Accueil. Vérifiez que la tâche affectée s'affiche dans votre liste de tâches.
2. Démarrez un processus planifié ou un opérateur. Vérifiez qu'il démarre à l'heure et se termine correctement.
3. Démarrez un processus avec des opérateurs exécutés sur des points de contact d'agent ou sur des hôtes distants via des points de contact du proxy. Vérifiez que l'instance de processus se termine correctement.
4. Autorisez l'utilisation de solutions se servant de CA Process Automation comme composant intégré à exécuter. Surveillez les résultats et vérifiez qu'aucun événement inattendu ne se produit.
5. Lorsque vous estimez que la nouvelle version de CA Process Automation qui utilise des communications simplifiées fonctionne comme prévu, reprenez l'ensemble de votre traitement habituel.

Chapitre 7: Réinstallation ou configuration de la version actuelle

Vous pouvez apporter des changements à la version de compilation actuelle de l'orchestrateur en réexécutant l'assistant d'installation. Les options incluent la réinstallation et la configuration de l'installation existante.

Ce chapitre traite des sujets suivants :

Exemple de scénario : configuration de l'installation existante pour régénérer les certificats CA Process Automation (page 162)
Prise en charge de la post-installation lors des mises à niveau de CA EEM (page 167)
Activation de la communication sécurisée pour la version existante de CA Process Automation (page 171)

Exemple de scénario : configuration de l'installation existante pour régénérer les certificats CA Process Automation

Lorsque vous exécutez le processus d'installation pour la version que vous avez installée préalablement, vous pouvez réinstaller ou configurer l'installation existante. Cet exemple de scénario présente l'utilisation de l'option Configurer l'installation existante pour régénérer les certificats que CA Process Automation utilise pour se connecter à CA EEM.

Le processus d'installation de l'orchestrateur de domaine vous permet d'enregistrer, ou de réenregistrer, CA Process Automation dans CA EEM. Ce processus d'enregistrement génère des certificats d'application pour CA Process Automation avec la même longueur de clé que les certificats utilisés par CA EEM.

Remarque : CA Process Automation comprend d'autres certificats qui ne sont pas affectés par l'enregistrement. Seuls les certificats que CA Process Automation utilise pour se connecter à CA EEM sont générés. L'emplacement des certificats est *répertoire_installation*/server/c2o/.c2orepository/public/certification.

La configuration suivante est utilisée dans cet exemple de scénario :

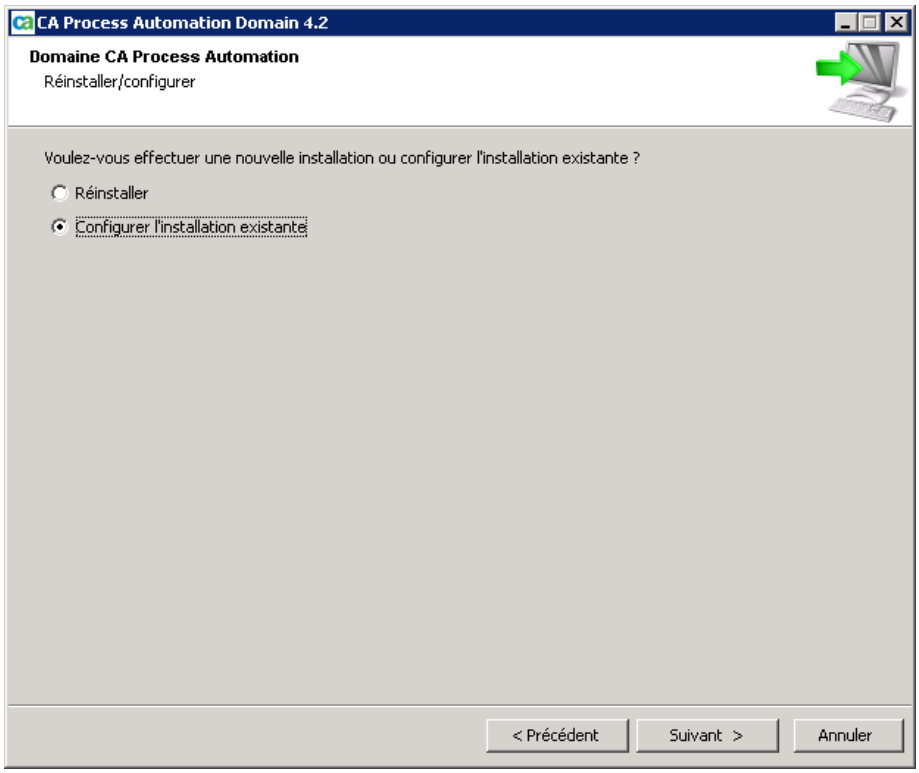
1. L'administrateur CA EEM installe ou met à niveau CA EEM vers la version 12.51 avec des certificats par défaut, dont la longueur de clé est de 1 024 bits.
2. Installez ou procédez à la mise à niveau vers CA Process Automation 4.2. Les certificats CA Process Automation générés ont également des clés de 1 024 bits.
3. L'administrateur CA EEM génère ultérieurement de nouveaux certificats CA EEM avec des longueurs de clé plus longues (2 048 ou 4 096 bits).

Dans ce cas, procédez comme suit pour régénérer des certificats CA Process Automation avec des longueurs clés qui correspondent à ceux des certificats CA EEM.

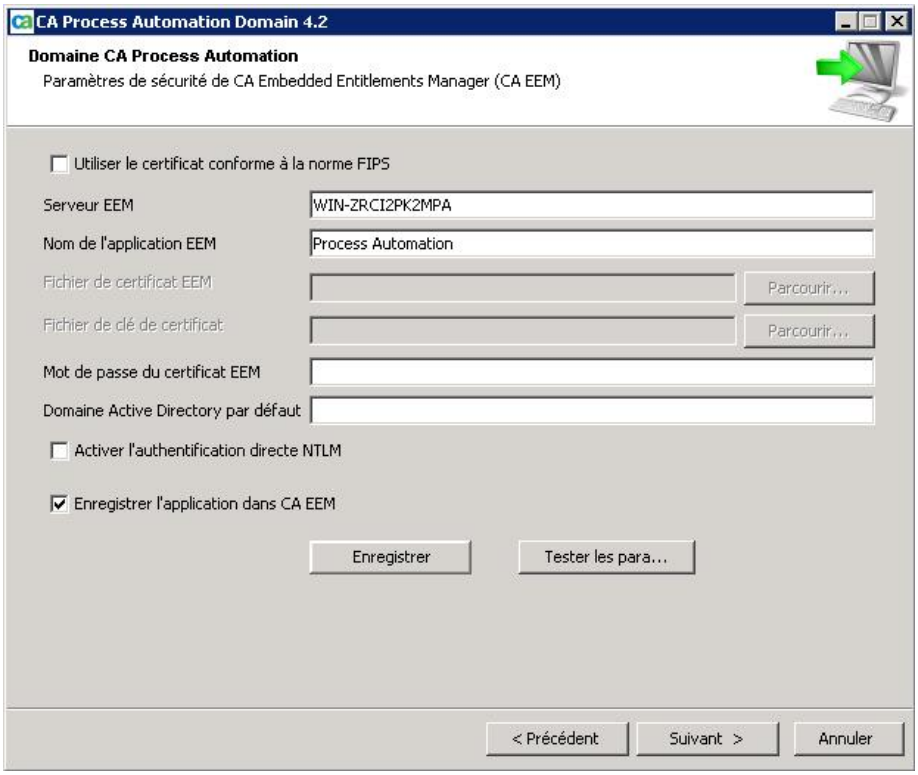
Procédez comme suit :

1. Installez les logiciels tiers. (page 94)

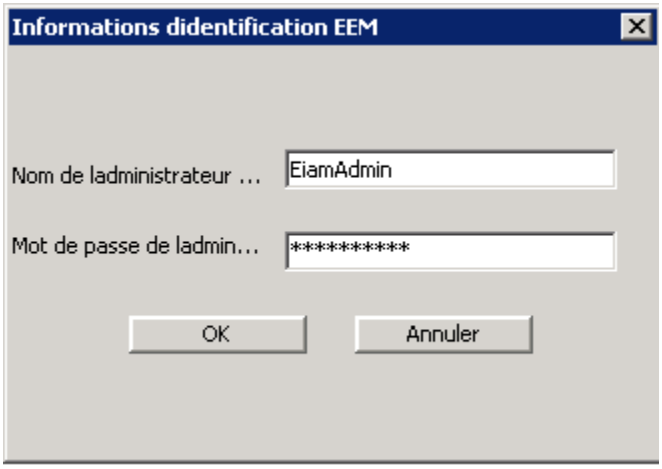
   Lorsque l'installation des logiciels tiers est terminée, le processus d'installation de domaine CA Process Automation démarre.
2. Passez les pages initiales jusqu'à ce que la page Réinstaller/configurer s'affiche.
3. Sélectionnez Configurer l'installation existante. (Ce processus modifie les fichiers de propriétés, mais ne modifie pas les fichiers JAR.)


CA Process Automation Domain 4.2
Domaine CA Process Automation
Réinstaller/configurer
Voulez-vous effectuer une nouvelle installation ou configurer l'installation existante ?
Réinstaller
Configurer l'installation existante
< Précédent
Suivant >
Annuler

4. Passez les pages jusqu'à ce que la page Paramètres de sécurité de CA Embedded Entitlements Manager (CA EEM) s'affiche.
5. Cochez la case Enregistrer l'application dans CA EEM, puis cliquez sur Enregistrer.

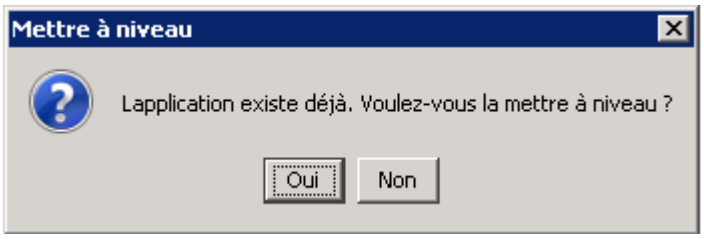


6. Entrez les informations d'identification de l'administrateur CA EEM. Saisissez **EiamAdmin** dans le champ Nom de l'administrateur EEM. Entrez le mot de passe associé.



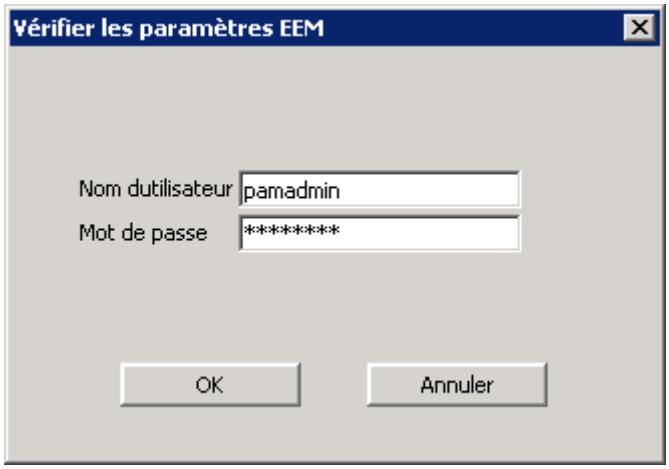
7. Cliquez sur Oui pour mettre à niveau l'application, même si vous ne mettez pas à niveau la version de CA Process Automation.

   (Cliquer sur Oui est obligatoire pour la génération des certificats d'application requis par CA Process Automation.)



8. Cliquez sur Tester les paramètres EEM. Cliquez sur OK lorsque les messages du programme d'installation s'affiche.
9. Entrez les informations d'identification d'un utilisateur CA Process Automation affecté au groupe PAMAdmins.

   Remarque : L'exemple d'entrée **pamadmin**, **pamadmin** est valide uniquement **si** vous avez configuré CA EEM pour utiliser le référentiel d'utilisateurs interne.



10. Vérifiez que CA Process Automation se connecte à CA EEM et que CA EEM authentifie les informations d'identification.

11. Passez le reste des étapes du processus d'installation, puis cliquez sur Terminer.

Prise en charge de la post-installation lors des mises à niveau de CA EEM

Si vous exécutez le processus d'installation pour la même version CA Process Automation, les options suivantes seront disponibles :

Réinstaller

Affiche l'assistant d'installation complet.

Sélectionnez Réinstaller si votre installation précédente utilisait un serveur CA EEM r8.4 que vous aviez mis à niveau vers la version 12.

- Si vous enregistrez l'application avec CA EEM 12.x, le processus de réinstallation sélectionne la version majeure 12 du kit de développement logiciel de CA EEM.
- Si vous n'enregistrez pas l'application, le processus de réinstallation vous invite à sélectionner un kit de développement logiciel approprié à votre version de CA EEM.

Sélectionnez l'option Réinstaller si vous utilisez CA EEM version 12.5 et si la version du kit de développement logiciel est la version majeure 8. Le processus de réinstallation met à jour le kit de développement logiciel vers la version majeure 12.

Remarque : CA Process Automation peut utiliser la version majeure 8 du kit de développement logiciel de CA EEM avec la version 12.x de CA EEM. La mise à niveau du kit de développement logiciel vers la version majeure 12 permet d'utiliser les nouvelles fonctionnalités de CA EEM.

Configurer l'installation existante

Affiche uniquement les pages sélectionnées. (Ce processus modifie les fichiers de propriétés, mais ne modifie pas les fichiers JAR.)

Sélectionnez cette option si vous avez généré des certificats de CA EEM dont les clés sont plus longues (2 048 ou 4 096 bits) ou après l'installation ou la mise à niveau de CA Process Automation vers la version 4.2.

Lorsque vous cliquez sur Enregistrer dans la page de configuration de CA EEM, CA Process Automation vous invite à mettre à niveau l'application existante dans CA EEM. Lorsque vous acceptez de procéder à la mise à niveau, les certificats de CA Process Automation utilisés pour communiquer avec CA EEM sont régénérés. Les nouveaux certificats de CA Process Automation ont des longueurs de clé correspondant aux longueurs des certificats de CA EEM.

Remarque : Pour plus d'informations sur la mise à niveau de CA EEM ou de ses certificats, consultez la documentation de CA EEM.

CA Process Automation utilise le kit de développement logiciel CA EEM pour communiquer avec CA EEM. Les communications sont sécurisées avec des certificats. CA EEM et CA Process Automation utilisent des certificats. Les certificats CA Process Automation doivent avoir la même longueur de clé que les certificats CA EEM.

Pendant l'installation de CA Process Automation 4.2 ou la mise à niveau vers la version 4.2, le programme d'installation récupère les certificats CA Process Automation de CA EEM et choisit le kit de développement logiciel approprié pour le serveur CA EEM associé. Les certificats se trouvent à l'emplacement suivant :

répertoire_installation/server/c2o/.c2orepository/public/certification

Si CA EEM n'est pas modifié, aucune action n'est requise. Toutefois, vous devez prendre certaines mesures si les modifications suivantes sont apportées à CA EEM.

Installez CA Process Automation 4.2 avec CA EEM 8.4, puis mettez à niveau CA EEM vers 12.x.

Si les certificats CA EEM sont générés avec les longueurs de clé par défaut, aucune action n'est requise et CA Process Automation peut être utilisé avec CA EEM. CA Process Automation peut utiliser la version majeure 8 du kit de développement logiciel CA EEM pour communiquer avec CA EEM 12.x. Toutefois, la version majeure 12 du kit de développement logiciel CA EEM vous permet de tirer parti des nouvelles fonctionnalités de CA EEM 12.x.

Il est donc recommandé de procéder à la mise à niveau des certificats utilisés par CA Process Automation pour communiquer avec CA EEM, puis de procéder à la mise à niveau de CA Process Automation pour utiliser la version majeure 12 du kit de développement logiciel CA EEM. Pour cela, réexécutez le programme d'installation. La procédure suivante référence les numéros d'étapes de la rubrique Installation de l'orchestrateur de domaine (page 96).

- Etape 5 : sélectionnez **Réinstaller** au lieu de Configurer l'installation existante.
- Etape 16 : cochez la case **Enregistrer l'application dans CA EEM.**
- Etape 17 : cliquez sur **Enregistrer**. A l'invite de confirmation de la mise à niveau, sélectionnez **Oui**, puis cliquez sur **OK** lorsque la confirmation Application enregistrée s'affiche.

Installez CA Process Automation 4.2 avec la CA EEM 12.51, puis générez de nouveaux certificats CA EEM avec des longueurs clés de 2 048 ou 4 096.

1. CA Process Automation 4.2 est installé avec CA EEM 12.51 à l'aide de certificats dont la longueur de clé est de 1 024 bits.
2. Générez de nouveaux certificats CA EEM avec des longueurs de clé de 2 048 ou 4 096 bits.
3. Réexécutez l'assistant d'installation de CA Process Automation, mais sélectionnez Configurer l'installation existante au lieu de Réinstaller.
4. Enregistrez CA Process Automation dans CA EEM. Enregistrez la valeur configurée du nom de l'application CA EEM dans CA EEM. Le processus d'enregistrement génère de nouveaux certificats CA Process Automation.

Résultat : les certificats utilisés par CA Process Automation lors de l'appel du kit de développement logiciel CA EEM 12.51 correspondent aux longueurs de clé utilisées par CA EEM.

Reportez-vous à la rubrique Exemple de scénario : configuration de l'installation existante pour régénérer les certificats CA Process Automation (page 162).

Configuration de CA EEM pour permettre aux utilisateurs référencés de se connecter avec une adresse électronique

1. CA Process Automation 4.2 est installé avec CA EEM à l'aide d'un référentiel d'utilisateurs référencé. Le référentiel d'utilisateurs référencé est configuré en tant que domaine Active Directory multiple.
2. Au cours de l'installation de CA Process Automation, vous définissez le domaine Active Directory à utiliser en tant que domaine Active Directory par défaut.

   Les utilisateurs référencés appartenant au domaine Active Directory par défaut peuvent se connecter à CA Process Automation avec leur nom d'utilisateur non qualifié et leur mot de passe.
3. Sans l'étape suivante, CA EEM autorise les utilisateurs référencés dans d'autres domaines à se connecter avec leur nom principal (*domaine\nom_utilisateur)* et leur mot de passe.
4. Configurez CA EEM pour permettre aux utilisateurs référencés de se connecter avec une adresse électronique. (page 132)

Résultat : les utilisateurs non référencés dans le domaine Active Directory configuré par défaut peuvent se connecter avec leur mot de passe et leur nom principal, dont les formats suivants sont pris en charge :

nom d'utilisateur@*domaine*

*domaine**nom d'utilisateur*

Récapitulatif de l'enregistrement de l'application dans CA EEM

- Si vous sélectionnez la case à cocher Enregistrer l'application dans CA EEM et qu'il ne s'agit pas d'une nouvelle installation, cliquez sur **Enregistrer**. Vous êtes invité à confirmer si vous voulez mettre à niveau l'application CA Process Automation.
  - Sélectionnez Oui pour procéder à la mise à niveau vers une nouvelle version.
  - Sélectionnez Oui pour générer de nouveaux certificats CA Process Automation dans le cadre de la configuration de l'installation existante.
  - Sélectionnez Non si vous réinstallez la même version et ne voulez pas régénérer les certificats.

Activation de la communication sécurisée pour la version existante de CA Process Automation

Si vous avez préalablement sélectionné HTTP comme protocole pour la communication de l'orchestrateur de domaine, vous pouvez à présent utiliser le protocole HTTPS pour une communication sécurisée.

Procédez comme suit :

1. Réinstallez l'orchestrateur de domaine. Spécifiez l'utilisation de communications sécurisées de l'une des façons suivantes, selon la méthode d'installation :
   - Si vous réinstallez l'orchestrateur de domaine interactivement (consultez la rubrique Installation de l'orchestrateur de domaine (page 96)), sélectionnez l'option Prise en charge des communications sécurisées.
   - Si vous créez un fichier de réponse pour l'installation de l'orchestrateur de domaine autonome, définissez la variable isSecure sur True pour activer les communications sécurisées via HTTPS :
     `isSecure=true`
2. Activez la communication sécurisée par des agents en suivant l'une des méthodes suivantes, en fonction de leur configuration.
   - Vérifiez que les agents configurés pour utiliser la communication désapprouvée redémarrent automatiquement. La communication désapprouvée est le paramètre par défaut des agents existants qui communiquent avec des orchestrateurs mis en cluster utilisant un équilibreur de charge Apache. Démarrez tous les agents (page 186) arrêtés avant la réinstallation.
   - Réinstallez les agents configurés pour utiliser la communication simplifiée. La communication simplifiée est le paramètre par défaut des nouveaux agents qui communiquent avec des orchestrateurs mis en cluster utilisant un équilibreur de charge NGINX. Réinstallez les agents comme indiqué dans la section Installation d'un agent (page 173). Puis, démarrez les agents (page 186).

   HTTPS est utilisé pour toutes les communications entre les agents et l'orchestrateur de domaine.
3. Vérifiez que toutes les instances de processus qui utilisent les pièces jointes SOAP existantes sont terminées.

   Remarque : Les pièces jointes SOAP existantes sont accessibles via HTTP uniquement.
4. Définissez des règles de pare-feu pour le blocage des communications HTTP.

Chapitre 8: Installation des agents

Ce chapitre traite des sujets suivants :

Conditions préalables à l'installation des agents (page 173)
Accès et connexion à CA Process Automation (page 175)
Installation interactive d'un agent (page 176)
Exécution d'une installation autonome d'agents (page 179)
Tâches de post-installation des agents (page 183)

Conditions préalables à l'installation des agents

Effectuez les opérations suivantes de préparation de l'installation d'un agent :

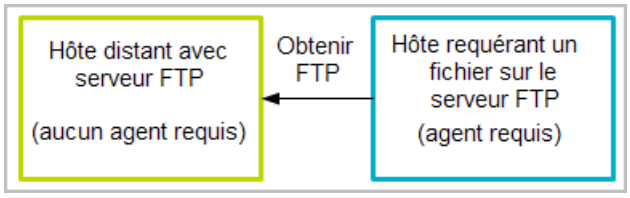
1. Identification des hôtes qui requièrent des agents (page 173)
2. Vérification de la configuration Java requise pour les agents (page 174)
3. Détermination de la disponibilité du port pour l'agent (page 174) (uniquement pour la communication désapprouvée)

Identification des hôtes qui ont besoin des agents

Dans la plupart des cas, les opérateurs s'exécutent sur un orchestrateur. En d'autres termes, l'opérateur cible le point de contact d'un orchestrateur. Les opérateurs s'exécutent également sur des hôtes avec agents. L'opérateur doit alors cibler un point de contact associé à un ou plusieurs agents.

Exemple : installation des agents sur des hôtes qui exécutent des opérateurs

En général, les agents CA Process Automation s'installent sur les hôtes sur lesquels les opérateurs sont exécutés et non pas sur les hôtes auxquels l'opérateur se connecte pendant l'exécution. Imaginons par exemple qu'un hôte a besoin d'un fichier sur le serveur FTP. L'hôte qui a besoin du fichier exécute l'opérateur FTP GET. Un agent doit être installé sur l'hôte sur lequel l'opérateur est en cours d'exécution. Aucun agent n'est requis sur l'hôte équipé avec le serveur FTP



Remarque : Lorsqu'il n'est pas possible d'installer un agent sur un hôte distant sur lequel un opérateur doit être exécuté, vous pouvez connecter un hôte équipé d'un agent à l'hôte distant à l'aide d'une connexion SSH. Pour plus d'informations sur les points de contact de proxy, reportez-vous au *Manuel de l'administrateur de contenu*.

Vérification des conditions Java requises pour les agents

Avant d'installer un agent sur un hôte, vérifiez que les conditions Java requises sont remplies.

Procédez comme suit :

1. Connectez-vous à l'hôte. Assurez-vous qu'une version du JRE (environnement d'exécution Java) prise en charge est installée. Si aucune version appropriée n'est installée, téléchargez le JRE directement à partir du site du fournisseur et procédez à l'installation.
2. (Facultatif) Définissez la variable d'environnement JAVA_HOME vers le chemin d'accès du JRE pour l'agent. Si cette variable n'est pas définie, le programme d'installation CA Process Automation invite l'utilisateur à accéder au répertoire d'installation du JRE.

Détermination des ports disponibles pour l'agent

Cette étape est uniquement requise pour les agents qui utilisent la communication désapprouvée. La communication simplifiée utilise les ports standard HTTP (port 80) et HTTPS (port 443).

Les agents et les orchestrateurs utilisent les ports suivants pour communiquer les uns avec les autres.

- Port d'orchestrateur : 7001
- Port d'agent : 7003

Lorsque vous installez un agent, vous devez configurer les ports qu'il utilise. Si vous configurez les ports réseau d'un agent, acceptez les paramètres par défaut sauf dans les cas suivants :

- Une autre application présente sur l'hôte utilise le port par défaut.
- Une restriction de pare-feu empêche la communication sur le port par défaut.

Pour utiliser un port autre que le port par défaut, sélectionnez un port valide, qui n'est pas déjà utilisé.

Accès et connexion à CA Process Automation

L'URL que vous utilisez pour accéder à CA Process Automation varie selon que l'orchestrateur de domaine est configuré avec un noeud (non mis en cluster) ou plusieurs noeuds (mis en cluster). Vous pouvez accéder directement à un serveur CA Process Automation non mis en cluster. Pour un serveur CA Process Automation mis en cluster, accédez à l'équilibreur de charge associé. Vous pouvez accéder à tous les orchestrateurs du domaine en lançant l'URL de l'orchestrateur de domaine ou de l'équilibreur de charge de l'orchestrateur de domaine.

Procédez comme suit :

1. Accédez à CA Process Automation.

   - Pour une communication sécurisée, utilisez la syntaxe suivante :
     `https://serveur:port/itpam`

     Exemples :
     `https://Orchestrator_host:8443/itpam`
     `https://loadBalancer_host:443/itpam`

   - Pour une communication de base, utilisez la syntaxe suivante :
     `http://serveur:port/itpam`

     Exemples :
     `http://Orchestrator_host:8080/itpam`
     `http://loadBalancer_host:80/itpam`

   La page de connexion à CA Process Automation s'ouvre.

2. Entrez les informations d'identification de votre compte d'utilisateur.

   Remarque : Si CA EEM est configuré pour référencer des utilisateurs à partir de plusieurs annuaires Microsoft Active Directory et CA Process Automation n'accepte pas votre nom d'utilisateur non qualifié, entrez votre nom principal au format *nom_domaine**nom_utilisateur*.

3. Cliquez sur Connexion.

   CA Process Automation ouvre. L'onglet Accueil s'affiche.

Informations complémentaires

A propos des communications d'agent (page 159)

Installation interactive d'un agent

Les processus peuvent inclure des opérateurs qui doivent être exécutés sur des serveurs équipés d'une application, d'une base de données ou du système cible. Si possible, installez un agent sur un serveur de ce type. Si cela n'est pas possible, installez l'agent sur un hôte qui peut se connecter à ce serveur à travers le protocole SSH.

Important : Avant d'installer un agent, vérifiez que l'orchestrateur de domaine s'exécute.

Procédez comme suit :

1. Cliquez sur l'onglet Configuration.
2. Cliquez sur la palette Installation.
3. Pour installer l'agent, cliquez sur Installer.

   Une boîte de dialogue s'affiche et indique la progression du téléchargement de l'application.
4. Si vous recevez un avertissement de sécurité, cliquez sur Exécuter.

   La boîte de dialogue de sélection de langue s'ouvre. La langue de l'ordinateur hôte est sélectionnée par défaut.
5. Cliquez sur OK ou sélectionnez une autre langue, puis cliquez sur OK.

   La page Bienvenue de l'assistant d'installation d'agent CA Process Automation s'affiche.
6. Cliquez sur Suivant.

   La page du contrat de licence s'affiche.
7. Prenez-en connaissance. Si vous êtes d'accord, cliquez sur J'accepte les termes de ce contrat de licence. Cliquez sur Suivant.

   La page Définissez le répertoire de base Java s'ouvre.
8. Si le répertoire de base Java affiché est incorrect, accédez au dossier du kit de développement Java (JRE).

   Toutes les plates-formes prennent en charge JRE 6. Windows prend en charge JRE 6 et 7.

   Exemple de chemin d'accès pour la plate-forme Windows :

   ```
   C:\Program Files\Java\jdk1.7.0_45
   ```

9. Cliquez sur Suivant.

   La page de sélection du répertoire de destination s'ouvre. Chemin d'accès par défaut sur les hôtes Windows :

   ```
   C:\Program Files\CA\PAM Agent
   ```

10. Pour accepter la valeur par défaut, cliquez sur Suivant ou saisissez un répertoire de destination pour le nouvel agent, puis cliquez sur Suivant.

    La page de sélection du dossier de menu Démarrer s'ouvre.

11. (Windows uniquement) Pour accepter l'agent CA Process Automation comme raccourci du menu Démarrer, cliquez sur Suivant ou saisissez un nouveau nom et cliquez sur Suivant.

    - (Facultatif) Créez des raccourcis pour tous les utilisateurs sur cet hôte.
    - (Facultatif) Ne pas créer de dossier dans le menu Démarrer

12. Examinez l'URL de domaine. Il s'agit de l'URL à partir de laquelle vous avez lancé l'installation de l'agent. Cliquez sur Suivant.

13. Si le domaine est sécurisé, indiquez un mot de passe.
14. Remplissez la page Propriétés générales, puis cliquez sur Suivant.
    a. Dans Hôte de l'agent, saisissez le nom d'hôte de l'agent. Ce nom identifie l'hôte à partir duquel vous avez lancé l'installation.
    b. Changez ou acceptez le nom d'affichage par défaut, c'est-à-dire le nom d'hôte.
    c. Si vous avez lancé l'installation d'agent à partir d'un hôte Windows, sélectionnez Installer en tant que service Windows.
    d. Pour imposer une nouvelle connexion pour chaque communication d'un orchestrateur vers un agent, sélectionnez Utiliser la communication désapprouvée.

       Il est recommandé de laisser cette case *décochée*. La méthode de communication simplifiée est la méthode par défaut préférée, car une connexion persistante est utilisée.
    e. Si vous avez sélectionné Utiliser la communication désapprouvée, acceptez 7003 comme valeur pour Port de l'agent, sauf si ce port est déjà utilisé. Si le port par défaut est utilisé, entrez un numéro de port non utilisé, tel que 57003, comme port sur lequel l'agent écoute les communications avec les orchestrateurs.

       Remarque : Si la communication désapprouvée n'est pas utilisée, les orchestrateurs utilisent une connexion de socket Web (établie par des agents) pour communiquer avec les agents. Les orchestrateurs utilisent le port 80 pour communiquer avec les agents via HTTP et le port 443 pour communiquer avec les agents via HTTPS.
    f. Sélectionnez Démarrer l'agent après l'installation.

       Le démarrage de l'agent permet d'afficher l'agent actif et de poursuivre sa configuration.
15. Pour accepter le répertoire temporaire par défaut pour l'exécution des scripts, cliquez sur Suivant ou indiquez le chemin d'accès de votre choix et cliquez sur Suivant.

    Remarque : Le chemin d'accès ne doit comprendre aucun espace.

    La page Définir la politique d'exécution de PowerShell s'affiche.

16. Effectuez la configuration selon l'une des méthodes suivantes :
    - Pour exécuter des scripts Windows PowerShell via cet agent :
        a. Cochez la case Définir la politique d'exécution PowerShell.
        b. Accédez à l'emplacement de l'hôte PowerShell si la valeur par défaut affichée n'est pas appropriée.
        c. Cliquez sur Suivant.
    - Si vous n'utilisez pas Windows PowerShell, cliquez sur Suivant.

    L'installation de l'agent démarre.
17. Cliquez sur Terminer.
18. (Windows uniquement) Lancez le service de l'agent. Cliquez sur Démarrer, Programmes, CA, Agent CA Process Automation, Démarrer le service de l'agent.
19. Dans l'onglet Configuration, cliquez sur la palette Explorateur de configurations,
20. Cliquez sur Actualiser. ou déconnectez-vous, puis reconnectez-vous.
21. Développez le noeud Agents et vérifiez que le nom de l'agent y est répertorié.

    Remarque : Pour utiliser l'hôte de l'agent comme cible, configurez un point de contact. Pour utiliser l'hôte de l'agent comme passerelle vers un hôte distant, configurez un point de contact du proxy.

Exécution d'une installation autonome d'agents

CA Process Automation prend en charge l'installation autonome d'agents, qui permet aux administrateurs d'installer des agents à distance sur un ordinateur hôte. Vous pouvez utiliser une installation autonome pour inclure l'agent dans la routine de configuration initiale pour la configuration de nouveaux ordinateurs hôtes. Vous pouvez également utiliser l'installation autonome pour prendre en charge l'installation à travers des solutions de livraison de logiciel.

Lorsque vous entrez l'URL de domaine sous la forme -VdomainUrl=*URL_domaine*, *URL_domaine* correspond à http(s):<*FQDN_orchestrateur_domaine*>:<*numéro_port*>.

Important : La valeur *URL_domaine* doit être saisie sans **/itpam/**.

Vous pouvez effectuer une installation d'agent autonome.

Procédez comme suit :

1. Connectez-vous en tant qu'administrateur au serveur sur lequel l'orchestrateur de domaine est installé.
2. Vérifiez que ce dernier est en cours d'exécution.

   Remarque : Pour installer correctement un agent, le programme d'installation autonome d'agents doit tout de même disposer d'une connectivité à l'orchestrateur de domaine.
3. Accédez au répertoire suivant :

   répertoire_installation/server/c2o/.c2orepository/media

   Le dossier multimédia inclut les fichiers suivants :

   - AgentInstaller
   - AgentInstaller.sh
   - AgentInstaller_64
   - AgentInstaller-hpux.sh
   - CA_PAM_Agent_unix.sh
   - CA_PAM_Agent_windows_32
   - CA_PAM_Agent_windows_64
4. Localisez les deux fichiers correspondant à votre système d'exploitation :
   - Windows 32 bits : AgentInstaller.bat et CA_PAM_Agent_windows_32.exe
   - Windows 64 bits : AgentInstaller_64.bat et CA_PAM_Agent_windows_64.exe
   - UNX et Linux : Agent Install.sh et CA_PAM_Agent_unix.sh
   - HP-UX : AgentInstaller-hpux.sh et CA_PAM_Agent_unix.sh
5. Copiez les deux fichiers correspondant à votre système d'exploitation dans un répertoire de l'hôte sur lequel vous voulez installer l'agent.
6. Connectez-vous à l'hôte sur lequel vous voulez installer l'agent, puis accédez au répertoire dans lequel vous avez copié le programme d'installation des agents et les fichiers wrapper.
7. (Facultatif) Pour afficher l'aide, exécutez le programme d'installation d'agents sans arguments.
8. Utilisez les arguments de ligne de commande suivants avec le programme d'installation d'agents :

   ```
   AgentInstaller.bat -VdomainUrl=domain_url -VacceptLicense=true
   [-option1 -option2 ...]
   AgentInstaller.sh -VdomainUrl=domain_url
   –VacceptLicense=true[-option1 -option2 ...]
   ```

Exemple :

```
-VdomainURL=https://domainserver.company.com:8443-VacceptLicens
e=true
```

```
-VdomainURL=http://domainserver.company.com:8080
```

Le programme d'installation d'agent accepte les options de ligne de commande suivantes :

–VlisteningAddress=*hostname*

Spécifie le nom de domaine complet ou l'adresse IP de l'ordinateur hôte sur lequel vous installez l'agent. Cela est requis si l'ordinateur hôte a plusieurs interfaces de réseau.

-VdisplayName=*display_name*

Spécifie le nom qui est affiché pour cet agent.

-VnodePort=*port_number*

Spécifie le port à utiliser sur l'hôte.

-VwinService=*boolean*

Pour installer l'agent en tant que service Windows, définissez la valeur sur True.

-Vsys.installationDir=*path*

Spécifie le chemin complet pour l'installation sur l'hôte.

-VstartAgent=*boolean*

Pour démarrer l'agent une fois l'installation terminée, définissez la valeur sur True.

-VjavaHome=*value*

Spécifie l'emplacement du dossier Java de base.

-Vscripts.tmpDir=*value*

Spécifie le répertoire temporaire d'exécution des scripts.

VcertPassword=*value*

Spécifie le mot de passe de certificat configuré dans l'orchestrateur de domaine. Cette valeur est requise quand vous utilisez SSL et/ou que vous travaillez en mode sécurisé.

VisLookUpDNSForIP=*boolean*

Définissez la valeur sur True pour rechercher le nom d'hôte de l'agent à partir de DNS.

jetty.ssl.ciphers=*value*

Liste des méthodes de chiffrement séparées par une virgule qui doivent être utilisées au cours des communications entre l'agent et l'orchestrateur de domaine.

-VsetPowerShellExecPolicy=*value*

L'exécution de scripts PowerShell sur la plate-forme Windows requiert que la politique d'exécution soit définie sur RemoteSigned. Pour exécuter des scripts PowerShell dans CA Process Automation, définissez la valeur de cette variable sur True.

-VpowerShellPath=*value*

Spécifie le chemin d'accès à PowerShell sur l'ordinateur hôte.

-VdeprecatedComms=*boolean*

Spécifie le mode de communication (page 159). Définissez la valeur sur True pour permettre la prise en charge du mode de communication désapprouvé. Définissez la valeur sur False pour permettre la prise en charge du nouveau mode de communication.

Tâches de post-installation des agents

Les tâches de post-installation des agents varient selon les circonstances.

- En cas de conflit des ports après l'installation d'un agent, vous pouvez résoudre le conflit de ports pour l'agent (page 184).
- Si votre site ne permet pas l'exécution d'agents avec des droits d'accès root, vous pouvez exécuter des programmes pour configurer les agents à exécuter en tant qu'utilisateur à faibles privilèges standard (page 185).
- Les agents installés avec CA Process Automation r4.2 utilisent par défaut la méthode de communication simplifiée. Pour plus d'informations sur la configuration des agents en vue de l'utilisation de la méthode de communication désapprouvée conjointement à un équilibreur de charge Apache, consultez le *Manuel de l'administrateur de contenu*. Si vous avez procédé à la mise à niveau vers la version 4.2 de CA Process Automation, consultez la rubrique sur la configuration des agents existants en vue d'utiliser la communication simplifiée.

Résolution du conflit de ports pour un agent

Si un port cesse d'être disponible suite à l'installation d'un agent, modifiez l'affectation du port en suivant l'une des approches suivantes :

- **Windows** :
  1. Accédez au répertoire suivant sur l'hôte sur lequel l'agent est installé :
     `répertoire_installation_agent\.config`
  2. Ouvrez le fichier suivant dans un éditeur :
     `OasisConfig.properties`
  3. Modifiez l'affectation de port suivante :
     `oasis.jxta.port=`
  4. Enregistrez le fichier. Fermez le fichier.
  5. Accédez au répertoire suivant sur le serveur sur lequel l'orchestrateur de domaine est installé :
     `répertoire_installation/server/c2o/.system`
  6. Supprimez le dossier .c2o, s'il existe.
- **UNIX ou Linux** : ajustez la configuration de démarrage.

Configuration des agents pour une exécution en tant qu'utilisateur à faibles privilèges standard

Les programmes décrits dans cette section s'appliquent à un agent installé sur un hôte avec un système d'exploitation Windows. Ces programmes permettent de réaliser les actions suivantes :

- Créez le compte d'utilisateur standard utilisé pour tous les agents CA Process Automation.
- Affectez à cet agent les droits requis dans l'hôte local.

Remarque : Le fonctionnement de ces programmes avec toutes les versions Windows n'a pas été validé.

Si ces programmes ne fonctionnent pas sur votre version Windows, configurez les paramètres manuellement. Dans les outils d'administration Windows, utilisez l'éditeur de politiques de groupe.

Avant de commencer, déterminez le compte d'utilisateur *user_name* ou *group_name* à utiliser par défaut sur tous les agents et orchestrateurs installés. Vous pouvez utiliser un compte d'utilisateur ordinaire. Il ne doit pas nécessairement s'agir d'un compte de domaine disposant de droits d'administration.

Procédez comme suit :

1. Ouvrez une invite de commande Vous pouvez par exemple exécuter cmd.
2. Accédez au répertoire suivant :

   répertoire_installation_agent\PAMAgent\.c2orepository\public\tools
3. Tapez la commande suivante :

   ```
   itpamsvcacct.bat user_name|group_name
   ```

   Le compte d'utilisateur est créé avec le nom spécifié.
4. Saisissez les cinq commandes suivantes. Vous pouvez saisir une seule commande et utiliser un espace comme délimiteur entre les droits.

   ```
   itpamassgnrights.exe user_name host_name + SeTcbPrivilege
   itpamassgnrights.exe user_name host_name + SeCreateTokenPrivilege
   itpamassgnrights.exe user_name host_name + SeServiceLogonRight
   itpamassgnrights.exe user_name host_name + SeBatchLogonRight
   itpamassgnrights.exe user_name host_name +
   SeAssignPrimaryTokenPrivilege
   ```

   Le compte d'utilisateur spécifié dispose des droits requis pour exécuter l'agent sur l'hôte local spécifié.

Démarrage et arrêt d'un agent

La méthode de démarrage et d'arrêt d'un agent dépend du système d'exploitation que l'hôte sur lequel est installé l'agent utilise.

- Démarrage d'un agent (page 186)
- Arrêt d'un agent (page 187)

Démarrage d'un agent

Utilisez la méthode de démarrage ou de redémarrage d'agent pour le système d'exploitation sur l'hôte contenant l'agent.

Démarrage ou redémarrage d'un agent sur un hôte Microsoft Windows

La procédure suivante s'applique à un agent dans votre domaine CA Process Automation qui réside sur un hôte exécutant un système d'exploitation Windows.

Procédez comme suit :

1. Connectez-vous à l'hôte Windows sur lequel un agent est installé.
2. Dans le menu Démarrer, sélectionnez Programmes, CA, Agent CA Process Automation, Démarrer le service de l'agent.
3. Déconnectez-vous de l'hôte.

Démarrage ou redémarrage d'un agent sur un hôte Linux

La procédure suivante s'applique à un agent dans votre domaine CA Process Automation qui réside sur un hôte exécutant un système d'exploitation UNIX ou Linux.

Procédez comme suit :

1. Connectez-vous à l'hôte UNIX ou Linux sur lequel un agent est installé.
2. Remplacez les répertoires par :

   ```
   usr/local/CA/PAMAgent/pamagent
   ```
3. Exécutez la commande suivante :

   ```
   ./c2oagtd.sh start
   ```

   L'agent redémarre.

Arrêt d'un agent

Vous pouvez arrêter un agent CA Process Automation exécuté sur un hôte UNIX ou Linux.

Arrêt d'un agent sur un hôte Microsoft Windows

La procédure suivante s'applique à un agent dans votre domaine CA Process Automation qui réside sur un hôte exécutant un système d'exploitation Windows.

Procédez comme suit :

1. Connectez-vous à l'hôte Windows sur lequel un agent est installé.
2. Dans le menu Démarrer, sélectionnez Programmes, CA, Agent CA Process Automation, Arrêter le service de l'agent.
3. Déconnectez-vous de l'hôte.

Arrêt d'un agent sur un hôte Linux

La procédure suivante s'applique à un agent dans votre domaine CA Process Automation qui réside sur un hôte exécutant un système d'exploitation UNIX ou Linux.

Procédez comme suit :

1. Connectez-vous à l'hôte UNIX ou Linux sur lequel un agent est installé.
2. Remplacez les répertoires par :

   ```
   usr/local/CA/PAMAgent/pamagent
   ```

3. Exécutez la commande suivante :

   ```
   ./c2oagtd.sh stop
   ```

   L'exécution de l'agent s'arrête.

Chapitre 9: Ajout d'un noeud à l'orchestrateur de domaine

Vous pouvez vous créer le domaine CA Process Automation en étendant la capacité de l'orchestrateur de domaine. L'ajout d'un noeud de cluster permet de bénéficier de la haute disponibilité au niveau de l'orchestrateur de domaine. Pour mettre à niveau un noeud, suivez le même processus utilisé pour ajouter un noeud.

Ce chapitre traite des sujets suivants :

Conditions préalables à l'installation d'un noeud de cluster pour l'orchestrateur de domaine (page 190)
Installez un noeud de cluster pour l'orchestrateur de domaine (page 193)
Synchronisation horaire d'un noeud de cluster (page 195)

Conditions préalables à l'installation d'un noeud de cluster pour l'orchestrateur de domaine

Vous pouvez installer un noeud de cluster pour l'orchestrateur de domaine. Les noeuds de cluster augmentent la puissance de traitement de l'orchestrateur de domaine et permettent donc d'en améliorer les performances. Les noeuds de cluster partagent les bases de données configurées pour les autres noeuds existants inclus dans le cluster d'orchestrateur de domaine.

Avant l'installation, effectuez les opérations suivantes :

Procédez comme suit :

1. Identifiez un hôte pour le noeud de cluster d'orchestrateur qui remplit les conditions au niveau de la plate-forme et du matériel. Pour en savoir plus sur le composant Orchestrateur, consultez les deux rubriques suivantes :
   - Prise en charge des plates-formes et conditions requises pour les composants CA Process Automation (page 30)
   - Configuration matérielle requise (page 32)
2. Vérifiez que l'hôte pour ce noeud de cluster appartient au même sous-réseau que les autres noeuds existants inclus dans l'orchestrateur de domaine.
3. Vérifiez que l'hôte pour ce noeud de cluster appartient au même fuseau horaire que les autres noeuds existants inclus dans l'orchestrateur de domaine.
4. Vérifiez que l'hôte de ce noeud de cluster est équipé d'un kit de développement Java pris en charge et, si ce n'est pas le cas, téléchargez ce kit JDK.

   Voir Configuration requise pour le kit de développement Java (page 77)
5. Si l'hôte pour le noeud de cluster exécute une version récente d'un système d'exploitation Windows, vérifiez l'option Contrôle de compte d'utilisateur (dans Panneau de configuration, Comptes d'utilisateurs). Si cette option est activée, décochez la case et redémarrez le serveur.

6. Si l'orchestrateur de domaine a été configuré avec un équilibreur de charge F5, ajoutez ce noeud à l'équilibreur de charge.

   Voir Création d'un noeud F5 pour chaque noeud de cluster (page 54).

7. Si l'orchestrateur de domaine a été configuré avec un équilibreur de charge Apache, ajoutez ce noeud à l'équilibreur de charge.

   a. Accédez au dossier *répertoire_installation_apache*\conf.

   b. Ouvrez le fichier workers.properties.

   c. Supprimer les marques de commentaire des lignes suivantes du fichier worker.properties, sous Define Node 2.

      ```
      worker.node2.port=8009
      worker.node2.host=nom_hôte
      worker.node2.type=ajp13
      worker.node2.lbfactor=1
      ```

   d. Remplacez *nom_hôte* par le nom d'hôte du serveur sur lequel le noeud Orchestrateur de domaine est installé.

   e. Ajoutez node2 à la ligne worker.loadbalancer.balance_workers= sous Load-balancing behaviour. Exemple d'entrée :

      ```
      worker.loadbalancer.balance_workers=node1,node2
      ```

      Remarque : Suivez ces instructions pour le troisième noeud et les noeuds suivants, mais adaptez le nombre de noeuds et remplacez node2 par node3 ou node4, par exemple.

   f. Redémarrez Apache.

8. Si le premier noeud de l'orchestrateur de domaine a été configuré avec un équilibreur de charge NGINX, ajoutez le noeud (node2) à l'équilibreur de charge.

   a. Accédez à l'emplacement du fichier pam-server.conf et ouvrez-le.

   b. Recherchez la ligne #Define node2. (Les données de node1 correspondent au premier noeud de l'orchestrateur de domaine. Ignorez les sections qui font référence au noeud node1)

      Remarque : *node2_hostname* correspond à l'adresse IP ou au nom DNS de l'hôte sur lequel le noeud node2 est installé. *port_serveur_jetty* correspond à la valeur de Port du serveur indiquée lors de l'installation du premier noeud de l'orchestrateur de domaine. Entrez 80 pour la communication simplifiée ou 7003 pour la communication désapprouvée.

   c. Créez les entrées suivantes dans pam-server.conf pour définir le noeud node1 et le nouveau noeud node2 :

      ```
      // node1 est le nom du noeud de travailleur.
      upstream node1{
        # Define node1
      ```

```
  server nom_hôte_node2:port_serveur_jetty max_fails=3
fail_timeout=3s;
}
// node2 est le nom du noeud de travailleur.
upstream node2{
  # Define node2
  server nom_hôte_node2:port_serveur_jetty max_fails=3
fail_timeout=3s;
}
```

d. Dans la balise server, créez les entrées suivantes pour les noeuds node1 et node2 :

```
Server{

...
    location = /ws {
                // node1 est le nom du noeud en amont fourni
ci-dessus.
                proxy_pass http://node1;
                }
    location = /ws/ {
                // node1 est le nom du noeud en amont fourni
ci-dessus.
                proxy_pass http://node1;
                }
    location = /ws/node1 {
                // node1 est le nom du noeud en amont fourni
ci-dessus.
                proxy_pass http://node1;
                }
    location /ws/node1/ {
                // node1 est le nom du noeud en amont fourni
ci-dessus.
                proxy_pass http://node1;
                }
    location = /ws/node2 {
                // node2 est le nom du noeud en amont fourni
ci-dessus.
                 proxy_pass http://node2;
                }
    location /ws/node2/ {
                // node2 est le nom du noeud en amont fourni
ci-dessus.
                proxy_pass http://node2;
                }
}
```

Installez un noeud de cluster pour l'orchestrateur de domaine

Les utilisateurs possédant des droits PAMAdmin peuvent également ajouter des noeuds de cluster supplémentaires à un orchestrateur de domaine. La mise en cluster permet d'équilibrer la charge de traitement sur l'ensemble d'hôtes mis en cluster. La mise en cluster est une bonne façon de promouvoir la haute disponibilité. Pour que l'orchestrateur de domaine soit éligible pour la mise en cluster, vous devoir avoir installé un équilibreur de charge avant d'avoir installé l'orchestrateur de domaine.

Vérifiez que les conditions préalables à l'installation d'un noeud de cluster pour l'orchestrateur de domaine (page 190) sont remplies, puis, installez le noeud de cluster.

Procédez comme suit :

1. Connectez-vous au serveur sur lequel vous envisagez d'installer le noeud de cluster pour l'orchestrateur de domaine.
2. Accédez à l'URL de l'orchestrateur de domaine et connectez-vous.

   `https://`*`Load-Balancer-hostname`*`:8443/itpam`

   `http://`*`Load-Balancer-hostname`*`:8080/itpam`
3. Cliquez sur l'onglet Configuration.
4. Cliquez sur la palette Installation.
5. Dans la section Installer le noeud de cluster pour l'orchestrateur de domaine, cliquez sur Installer.
6. Si vous ne pouvez pas vérifier la signature numérique, cliquez sur Exécuter pour démarrer l'installation.
7. Dans la page Bienvenue dans l'assistant de configuration du programme d'installation de composants tiers CA Process Automation, cliquez sur Suivant.
8. Acceptez le contrat de licence et cliquez sur Suivant.
9. Spécifiez le répertoire de destination pour installer le noeud d'orchestrateur, puis cliquez sur Suivant.

   Le programme d'installation crée le dossier automatiquement s'il n'existe pas.
10. Dans la fenêtre Conditions préalables à l'installation de CA Process Automation, cliquez sur Suivant.

    La fenêtre Fin de l'assistant d'installation de CA Process Automation affiche une case à cocher Utiliser un domaine, ainsi qu'un chemin d'accès. Vérifiez que cette case est cochée. Le processus d'installation utilise les informations collectées à partir de l'installation de l'orchestrateur de domaine. Il n'est généralement pas nécessaire de modifier la valeur de cette case à cocher pendant l'installation, mais si vous avez besoin d'entrer de nouvelles informations, activez-la et entrez les nouvelles informations.
11. Pour lancer l'installation du noeud de cluster pour l'orchestrateur de domaine, cliquez sur Terminer.

12. Dans la fenêtre de bienvenue, cliquez sur Suivant.
13. Acceptez le contrat de licence et cliquez sur Suivant.
14. Utilisez le chemin d'accès indiqué ou naviguez jusqu'au répertoire de base Java. Cliquez sur Suivant.

    Le kit de développement Java est validé et l'installation de l'orchestrateur commence. La copie des fichiers de configuration ne prend qu'une minute.
15. Renseignez la fenêtre Configuration, puis cliquez sur Suivant.

    orchestrateur

    Spécifie l'orchestrateur auquel le noeud de cluster doit être ajouté. L'orchestrateur sélectionné dans la liste déroulante doit être configuré avec un nom d'hôte public indiquant le nom de domaine complet du serveur sur lequel l'équilibreur de charge est installé.

    Noeud de travail de l'équilibreur de charge

    Spécifie le nom de noeud, par exemple, node2. Le nom de ce noeud est indiqué dans le fichier workers.properties d'Apache, où *hostname* correspond au nom de l'hôte sur lequel vous installez le noeud de cluster :

    worker.**node2**.host=*hostname*.*mycompany*.com

    Remarque : La première installation de l'orchestrateur de domaine est node1. Pour le deuxième noeud, saisissez **node2.**
16. Affichez le nom de société et cliquez sur Suivant.
17. Entrez le mot de passe de certificat et cliquez sur Suivant.

    Mot de passe du certificat

    Indique le *même* mot de passe de certificat saisi lors de l'installation des noeuds précédents de l'orchestrateur de domaine.
18. Vérifiez les entrées dans les propriétés générales de l'orchestrateur. La plupart des paramètres sont ceux de l'installation de l'orchestrateur de domaine. Cliquez sur Suivant.

    Hôte de serveur

    Spécifie le nom de domaine complet de l'hôte où ce noeud de cluster pour l'orchestrateur de domaine est installé.
19. Spécifiez un dossier du menu Démarrer et cliquez sur Suivant.
20. Affichez les paramètres PowerShell.
21. Affichez les paramètres de sécurité de CA EEM, puis cliquez sur Suivant.
22. Affichez les paramètres de la base de données de référentiel (de bibliothèque) et cliquez sur Suivant.
23. Affichez les paramètres de la base de données d'exécution et cliquez sur Suivant.
24. Affichez les paramètres de la base de données de reporting et cliquez sur Suivant.

25. Surveillez les messages de progression au fur et à mesure de l'installation du noeud de cluster pour l'orchestrateur de domaine sur l'ordinateur sur lequel vous avez initialisé l'installation.
26. Cliquez sur Terminer.

    Le noeud de cluster de l'orchestrateur de domaine est installé.

Synchronisation horaire d'un noeud de cluster

Tous les noeuds de cluster d'un orchestrateur doivent marquer le même temps horloge, synchronisé avec un serveur de synchronisation externe standard. Utilisez l'une des approches suivantes pour synchroniser l'heure de tous les noeuds d'un cluster :

- Synchronisez tous les orchestrateurs et les noeuds de cluster vers un serveur de synchronisation externe standard (procédure préférée).
- Synchronisez manuellement l'heure de tous les noeuds de cluster supplémentaires, comme suit :
  1. Vérifiez l'exactitude de l'heure de tous les noeuds de cluster.
  2. Exécutez la commande de système d'exploitation appropriée sur chaque noeud de cluster pour synchroniser l'heure de l'ensemble des noeuds de cluster.

Chapitre 10: Installation d'un orchestrateur supplémentaire

Après avoir installé l'orchestrateur de domaine, vous pouvez installer des orchestrateurs supplémentaires afin de créer le domaine. Vous pouvez installer plusieurs orchestrateurs au sein d'un même environnement. Si vous créez un environnement en vue de son utilisation dans un environnement de production par exemple, installez un orchestrateur dans cet environnement.

Ce chapitre traite des sujets suivants :

Conditions préalables à l'installation d'un orchestrateur (page 197)
Installation d'un orchestrateur (page 200)
Tâches de post-installation d'un orchestrateur (page 206)

Conditions préalables à l'installation d'un orchestrateur

Vous pouvez installer un orchestrateur dans l'environnement dans lequel se trouve l'orchestrateur de domaine ou dans un environnement distinct. Avant d'installer un orchestrateur, effectuez les opérations préalables suivantes :

Procédez comme suit :

1. Identifiez un hôte pour l'orchestrateur qui remplit les conditions au niveau de la plate-forme et du matériel. Pour en savoir plus sur le composant Orchestrateur, consultez les deux rubriques suivantes :
   - Prise en charge des plates-formes et conditions requises pour les composants CA Process Automation (page 30)
   - Configuration matérielle requise (page 32)
2. Vérifiez que l'hôte de l'orchestrateur est équipé d'un kit de développement Java pris en charge et, si ce n'est pas le cas, téléchargez ce kit JDK.

   Voir Configuration requise pour le kit de développement Java (page 77)

3. Ayez à portée de main le mot de passe de certificat qui correspond au mot de passe du magasin de clés sur l'orchestrateur de domaine. Ce mot de passe contrôle l'accès aux clés utilisées pour chiffrer des mots de passe et d'autres données critiques.

   Important : Sans ce mot de passe, vous ne pourrez pas installer d'autres orchestrateurs.

4. Identifiez le serveur de base de données ou les serveurs devant héberger la base de données d'exécution et, le cas échéant, la base de données de référentiel (bibliothèque) pour cet orchestrateur. Tenez compte des restrictions suivantes :

   - Chaque orchestrateur doit posséder sa propre base de données d'exécution.
   - Un orchestrateur peut utiliser la base de données de bibliothèque de l'orchestrateur de domaine ou posséder sa propre base de données.
   - Généralement, tous les orchestrateurs du domaine utilisent la base de données de reporting créée pour l'orchestrateur de domaine.
   - Les serveurs de base de données doivent remplir les conditions requises au niveau de la plate-forme et du matériel. Pour en savoir plus sur le composant Serveur de base de données, consultez les deux rubriques suivantes :
     - Prise en charge des plates-formes et conditions requises pour les composants CA Process Automation (page 30)
     - Configuration matérielle requise (page 32)

5. Préparez le serveur de base de données. Vous pouvez créer les bases de données d'exécution et de référentiel sur des serveurs de base de données différents.

   Voir Conditions requises pour le serveur de base de données (page 69)

6. Déterminez si un équilibreur de charge est nécessaire pour cet orchestrateur. CA Process Automation prend en charge les méthodes d'équilibrage des orchestrateurs mis en cluster suivantes.

   Remarque : Il est recommandé d'utiliser un équilibreur de charge matérielle. Voir Conditions requises pour l'équilibreur de charge F5 (page 53) Si cela n'est pas possible, il est recommandé de choisir NGINX comme équilibreur de charge logicielle. NGINX pour UNIX s'adapte très facilement. NGINX pour Windows peut prendre en charge jusqu'à 300 agents à l'aide de la communication simplifiée. Voir Conditions requises pour l'équilibreur de charge NGINX

7. Si vous souhaitez mettre en cluster cet orchestrateur à l'aide de NGINX, effectuez les opérations complémentaires suivantes :

   a. Accédez à l'emplacement du fichier pam-server.conf et ouvrez-le.

   b. Recherchez la ligne #Define node1. (Les données de node1 correspondent au premier noeud d'orchestrateur installé.)

   c. Insérez les éléments suivants, où *port_serveur_jetty* correspond à la valeur configurée lors de l'installation pour le port du serveur. En général, les valeurs sont 80 pour la méthode de communication simplifiée ou 7003 si les agents qui se connectent à l'orchestrateur utilisent la méthode de communication désapprouvée.

```
// node1 est le nom du noeud de travailleur.
upstream node1{
  # Define node1
  server nom_hôte_node1:port_serveur_jetty max_fails=3
fail_timeout=3s;
}
```

   d. Dans la balise Server, créez les entrées suivantes :

```
Server{
       location = /ws {
                // node1 est le nom du noeud en amont fourni
ci-dessus.
                proxy_pass http://node1;
                }
       location = /ws/ {
                // node1 est le nom du noeud en amont fourni
ci-dessus.
                proxy_pass http://node1;
                }
       location = /ws/node1 {
                 // node1 est le nom du noeud en amont fourni
ci-dessus.
                proxy_pass http://node1;
                }
```

```
        location /ws/node1/ {
                // node1 est le nom du noeud en amont fourni
ci-dessus.
                proxy_pass http://node1;
                }
...
                }
}
```

8. Identifiez un serveur de synchronisation (serveur NTP). La configuration des orchestrateurs pour qu'ils utilisent tous le même serveur de synchronisation externe (ou serveur de synchronisation local) est la meilleure façon d'assurer la synchronisation.
9. Assurez-vous que les éléments suivants ont été démarrés avant d'accéder à CA Process Automation pour commencer l'installation d'un orchestrateur :
   - CA EEM
   - L'équilibreur de charge, si utilisé.
   - Le service Orchestrateur de domaine.
   - Le serveur de base de données que vous envisagez d'utiliser pour la base de données d'exécution ainsi qu'une base de données de référentiel (ou de bibliothèque) distincte.

Installation d'un orchestrateur

Une fois l'orchestrateur de domaine installé, vous pouvez ajouter des orchestrateurs sur d'autres hôtes. Chaque nouvel environnement doit inclure au moins un orchestrateur. Toutefois, l'utilisation de plusieurs orchestrateurs rend possible la segmentation. Les nouveaux orchestrateurs héritent des informations CA EEM à partir de l'orchestrateur de domaine.

Avant de réaliser la procédure suivante, assurez-vous de respecter les conditions préalables à l'installation d'un orchestrateur (page 197). Par exemple, vérifiez qu'un kit de développement Java est installé.

Pour installer un orchestrateur ou mettre à niveau un Orchestrateur existant, suivez la procédure suivante.

Procédez comme suit :

1. Connectez-vous au serveur sur lequel installer le nouvel orchestrateur.
2. Accédez à CA Process Automation, puis connectez-vous (page 175) avec les informations d'identification de l'administrateur. Par exemple, connectez-vous comme membre du groupe PAMAdmins.
3. Cliquez sur l'onglet Configuration et sélectionnez la palette Installation.

4. Cliquez sur le lien des conditions préalables et vérifiez qu'elles sont toutes remplies.
5. Cliquez sur Installer un orchestrateur.

   Si vous utilisez le navigateur Web Firefox, ouvrez-le avec le lanceur Java Web Start (disponible par défaut).

   Si nécessaire, installez le certificat requis en procédant comme indiqué.
   L'application se télécharge. La boîte de dialogue Sélectionner une langue peut s'afficher dans la barre d'état système.
6. Sélectionnez une langue, puis cliquez sur OK.

   La page Bienvenue dans l'assistant de configuration du programme d'installation de composants tiers CA Process Automation s'affiche.
7. Cliquez sur Suivant.
8. Acceptez le contrat de licence et cliquez sur Suivant.
9. Acceptez le répertoire d'installation par défaut (install_dir) ou modifiez-le et cliquez sur Suivant.
10. Cliquez sur Suivant dans la page Conditions préalables à l'installation de CA Process Automation.

    La page Installation de JBoss en cours montre la progression de l'installation de jboss-5.1.
11. Indiquez les fichiers JAR JDBC à installer en procédant de l'une des façons suivantes :

    - Désélectionnez la case à cocher Utiliser un domaine et cliquez sur Suivant. Cela permet d'indiquer d'utiliser les fichiers .jar JDBC configurés lors de l'installation de l'orchestrateur de domaine.
    - Procédez comme suit :

      a. Décochez la case Utiliser un domaine.

      b. Cliquez sur Ajouter des fichiers.

      c. Sélectionnez le type de serveur de base de données.

      d. Cliquez sur Parcourir et accédez au fichier JAR JDBC correspondant au type de serveur sélectionné.

      e. Cliquez sur Suivant.
12. Dans la fenêtre de confirmation, cliquez sur Suivant.
13. Pour passer au programme d'installation de CA Process Automation, cliquez sur Terminer.
14. Dans la fenêtre de bienvenue, cliquez sur Suivant.
15. Acceptez le contrat de licence et cliquez sur Suivant.

16. Réalisez l'une des actions suivantes dans la page Répertoire d'accueil Java :
    - Pour accepter la valeur par défaut, cliquez sur Suivant.
    - Accédez à l'emplacement du kit de développement Java et cliquez sur Suivant.
17. Affichez l'URL du domaine et cliquez sur Suivant.
18. Si vous n'utilisez pas l'authentification unique sur un équilibreur de charge, cliquez sur Suivant et ignorez l'étape suivante.
19. Renseignez la page qui apparaît et cliquez sur Suivant.

    Configurer l'authentification unique

    Spécifie si vous utilisez CA SiteMinder avec l'authentification unique, la valeur par défaut étant désélectionnée. La sélectionnez de cette option permet d'activer les champs suivants :
    - Type d'authentification unique (en-tête)
    - Paramètre d'authentification unique (utilisateur CA SM)
    - Type de serveur (nouvel orchestrateur)

    Configurer l'équilibreur de charge

    Spécifie si cet orchestrateur doit être installé de manière à être mis en cluster.

    Option activée

    Indique qu'un équilibreur de charge est configuré pour cet orchestrateur.

    Option désactivée

    Indique qu'aucun équilibreur de charge n'est configuré pour cet orchestrateur.

    Noeud de travail de l'équilibreur de charge (Apache)

    Spécifie le nom de ce noeud. Etant donné que cet orchestrateur est le premier noeud de ce cluster, indiquez **node1**.

    Remarque : Pour les noeuds autres que node1 (par exemple, node 2), reportez-vous aux sections suivantes :
    - Ajout d'un noeud à l'orchestrateur de domaine (page 189)
    - Ajout d'un noeud à un orchestrateur supplémentaire (page 207)

Nom d'hôte public

Spécifie le nom d'hôte public comme dans l'exemple suivant :

loadbalancerhost.*mycompany*.com

- Si l'orchestrateur de domaine utilise l'authentification unique, ce champ spécifie le nom de domaine complet de l'application IIS (Internet Information Services) ou Apache avec l'agent Web CA SiteMinder.
- Dans le cas contraire, ce champ spécifie le nom de domaine complet de l'équilibreur de charge.

Numéro de port d'hôte public

Si la case Prise en charge des communications sécurisées est décochée, ce champ spécifie le port HTTP de l'hôte public (IIS ou Apache).

Par défaut

80

Port d'hôte public sécurisé

Si la case Prise en charge des communications sécurisées est cochée, ce champ spécifie le port HTTPS de l'hôte public (IIS ou Apache).

Par défaut

443

Prise en charge des communications sécurisées

Spécifie si l'hôte public utilise HTTPS pour les communications sécurisées.

Option activée

L'hôte public utilise HTTPS pour les communications sécurisées.

Option désactivée

L'hôte public n'utilise pas HTTPS pour les communications sécurisées, mais HTTP pour la communication de base.

20. Affichez le nom de société et cliquez sur Suivant.
21. Saisissez le mot de passe de certificat utilisé par l'orchestrateur de domaine et cliquez sur Suivant.

    Si vous perdez ou oubliez ce mot de passe de certificat, vous devrez réinstaller tous les orchestrateurs dans le système CA Process Automation, en commençant par l'orchestrateur de domaine.

22. Spécifiez les préférences du dossier du menu Démarrer et cliquez sur Suivant.
23. Entrez les propriétés générales de l'orchestrateur et cliquez sur Suivant.

    Hôte de serveur

    Spécifie le nom de domaine complet de cet orchestrateur.

    Nom d'affichage

    Spécifie le nom que l'explorateur de configurations affiche pour cet orchestrateur.

    - Si vous ne configurez aucun équilibreur de charge, le nom d'affichage correspond au nom d'hôte du serveur.
    - Sinon, le nom d'affichage correspond au nom de domaine complet du serveur qui héberge l'équilibreur de charge.
24. Acceptez la valeur par défaut ou définissez le répertoire temporaire dans lequel exécuter les scripts, puis cliquez sur Suivant.
25. Définissez la politique d'exécution PowerShell et cliquez sur Suivant.
26. Entrez les paramètres de la base de données de référentiel correspondant à cet orchestrateur en procédant de l'une des façons suivantes :
    - Pour partager la base de données de référentiel (bibliothèque) que l'orchestrateur de domaine utilise, procédez comme suit :
        a. Entrez les informations que vous avez configurées pour l'orchestrateur de domaine.
        b. Cliquez sur Tester les paramètres de la base de données,
        c. Cliquez sur Suivant.
    - Pour créer un base de données de référentiel (bibliothèque) distincte pour cet orchestrateur, procédez comme suit :
        a. Remplissez tous les champs.
        b. Attribuez un nom unique à la base de données de référentiel.
        c. Cliquez sur Créer une base de données
        d. Cliquez sur Tester les paramètres de la base de données.
        e. Cliquez sur Suivant.

27. Entrez les paramètres de la base de données d'exécution. Chaque orchestrateur requiert une base de données d'exécution distincte.
    a. Si la nouvelle base de données d'exécution réside sur le même serveur de base de données que la base de données de référentiel de cet orchestrateur, cliquez sur Copier à partir du référentiel principal pour copier le nom d'utilisateur et le mot de passe définis.
    b. Si le serveur de base de données que vous spécifiez héberge d'autres bases de données d'exécution, attribuez un nom valide unique à cette base de données d'exécution.
    c. Cliquez sur Créer une base de données
    d. Cliquez sur Tester les paramètres de la base de données,
    e. Cliquez sur Suivant.
28. Affichez les paramètres de la base de données de reporting, puis cliquez sur Suivant. Tous les orchestrateurs du domaine partagent la même base de données de reporting.
29. Cliquez sur Terminer.

Tâches de post-installation d'un orchestrateur

Effectuez les tâches de post-installation suivantes si elles s'avèrent nécessaires.

1. Pour configurer un équilibreur de charge Apache en vue de l'utilisation de la communication sécurisée via SSL, procédez comme suit :
   a. Accédez au dossier suivant :
   répertoire_installation_apache\conf\extra\
   b. Ouvrez le fichier suivant :
   `httpd-ssl.conf`
   c. Ajoutez les lignes suivantes à la fin du fichier, entre les balises de <VirtualHost> </VirtualHost> :

   ```
   SSLOptions +StdEnvVars +ExportCertData
   JkMount /* loadbalancer
   ```

   Remarque : Pour configurer un équilibreur de charge dans le cadre de l'utilisation de la communication de base, insérez un commentaire dans l'instruction précédente.
   d. Enregistrez le fichier. Fermez le fichier.
   e. Redémarrez le serveur HTTP Apache.
2. Configuration des ports (page 93)
3. Activation de la communication bidirectionnelle au niveau du pare-feu (page 129)
4. Si vous avez installé l'orchestrateur de domaine sur un serveur équipé du système d'exploitation HP-UX, effectuez les étapes de configuration supplémentaires requises sous HP-UX.
5. (Windows uniquement) Lancez le service de l'orchestrateur.

   L'orchestrateur s'inscrit lui-même auprès de l'orchestrateur de domaine.
6. Vérifiez l'installation de l'orchestrateur supplémentaire.
   a. Accédez et connectez-vous à CA Process Automation.
   b. Cliquez sur l'onglet Configuration.
   c. Cliquez sur le noeud Orchestrateurs dans la palette Explorateur de configurations.
   d. Le nouvel orchestrateur est affiché dans la liste.

Chapitre 11: Ajout d'un noeud à un orchestrateur supplémentaire

Après avoir installé un orchestrateur supplémentaire, vous pouvez étendre sa capacité et lui ajouter une fonctionnalité de basculement en ajoutant un noeud de cluster. Si un noeud échoue, un autre noeud prend le contrôle. L'installation des noeuds de cluster peut être interactive ou autonome.

Ce chapitre traite des sujets suivants :

Conditions préalables à l'installation d'un noeud de cluster pour un orchestrateur (page 208)
Installation d'un noeud de cluster pour un orchestrateur (page 211)
Synchronisation horaire d'un noeud de cluster (page 213)

Conditions préalables à l'installation d'un noeud de cluster pour un orchestrateur

Vous pouvez installer un noeud de cluster pour un orchestrateur. Les noeuds de cluster augmentent la puissance de traitement d'un orchestrateur et permettent donc d'en améliorer les performances. Les noeuds de cluster partagent les bases de données configurées pour les autres noeuds existants inclus dans le cluster d'orchestrateur.

Avant l'installation, effectuez les opérations suivantes :

Procédez comme suit :

1. Identifiez un hôte pour le noeud de cluster d'orchestrateur qui remplit les conditions au niveau de la plate-forme et du matériel. Pour en savoir plus sur le composant Orchestrateur, consultez les deux rubriques suivantes :
   - Prise en charge des plates-formes et conditions requises pour les composants CA Process Automation (page 30)
   - Configuration matérielle requise (page 32)
2. Vérifiez que l'hôte pour ce noeud de cluster appartient au même sous-réseau que les autres noeuds existants inclus dans l'orchestrateur.
3. Vérifiez que l'hôte pour ce noeud de cluster appartient au même fuseau horaire que les autres noeuds existants inclus dans l'orchestrateur.
4. Vérifiez que l'hôte de ce noeud de cluster est équipé d'un kit de développement Java pris en charge et, si ce n'est pas le cas, téléchargez ce kit JDK.

   Voir Configuration requise pour le kit de développement Java (page 77)
5. Si l'hôte pour le noeud de cluster exécute une version récente d'un système d'exploitation Windows, vérifiez l'option Contrôle de compte d'utilisateur (dans Panneau de configuration, Comptes d'utilisateurs). Si cette option est activée, décochez la case et redémarrez le serveur.

6. Si l'orchestrateur a été configuré avec un équilibreur de charge F5, ajoutez ce noeud à l'équilibreur de charge.

   Voir Création d'un noeud F5 pour chaque noeud de cluster (page 54).

7. Si l'orchestrateur a été configuré avec un équilibreur de charge Apache, ajoutez ce noeud à l'équilibreur de charge.

   a. Accédez au dossier *répertoire_installation_apache*\conf.

   b. Ouvrez le fichier workers.properties.

   c. Supprimer les marques de commentaire des lignes suivantes du fichier worker.properties, sous Define Node 2.

      ```
      worker.node2.port=8009
      worker.node2.host=nom_hôte
      worker.node2.type=ajp13
      worker.node2.lbfactor=1
      ```

   d. Remplacez *nom_hôte* par le nom d'hôte du serveur sur lequel le noeud Orchestrateur est installé.

   e. Ajoutez node2 à la ligne de worker.loadbalancer.balance_workers= sous Load-balancing behaviour. Exemple d'entrée :

      ```
      worker.loadbalancer.balance_workers=node1,node2
      ```

      Remarque : Suivez ces instructions pour le troisième noeud et les noeuds suivants, mais adaptez le nombre de noeuds et remplacez node2 par node3 ou node4, par exemple.

   f. Redémarrez Apache.

8. Si l'orchestrateur a été configuré avec un équilibreur de charge NGINX, ajoutez ce noeud à l'équilibreur de charge.

   a. Accédez à l'emplacement du fichier pam-server.conf et ouvrez-le.

   b. Recherchez la ligne #Define node2. (Les données de node1 correspondent au premier noeud de l'orchestrateur. Ignorez les sections qui font référence au noeud node1)

   c. Insérez les éléments suivants :

      ```
      # Define node2
        server nom_hôte_node2:port_serveur_jetty max_fails=3
      fail_timeout=3s;
      }
      ```

      Remarque : Le port de serveur Jetty correspond à la valeur de Port du serveur indiquée lors de l'installation du premier noeud de l'orchestrateur de domaine. Entrez 80 pour la communication simplifiée ou 7003 pour la communication désapprouvée.

      Dans la balise Server, créez les entrées suivantes :

      ```
      Server{
      ```

```
     location = /ws {
...
                // node2 est le nom du noeud en amont fourni
ci-dessus.
                proxy_pass http://node2;
                }
     location /ws/node2/ {
                // node2 est le nom du noeud en amont fourni
ci-dessus.
                proxy_pass http://node2;
                }
}
```

Installation d'un noeud de cluster pour un orchestrateur

Les utilisateurs possédant des droits PAMAdmins peuvent ajouter des noeuds de cluster supplémentaires à un orchestrateur équipé d'un équilibreur de charge.

Vérifiez que les conditions préalables à l'installation d'un noeud de cluster pour l'orchestrateur (page 208) sont remplies, puis, installez le noeud de cluster. Cette même procédure est utilisée pour mettre à niveau un noeud de cluster vers une nouvelle version.

Procédez comme suit :

1. Connectez-vous au serveur sur lequel vous souhaitez installer le noeud de cluster pour un orchestrateur supplémentaire.
2. Accédez à l'orchestrateur auquel vous voulez ajouter le noeud de cluster et vous connecter.

   `https://`*`Load-balancer-hostname`*`:8443/itpam`

   `http://`*`Load-balancer-hostname`*`:8080/itpam`
3. Cliquez sur l'onglet Configuration et sélectionnez la palette Installation.
4. Dans la section *Installer le noeud de cluster pour l'orchestrateur*, cliquez sur Installer.
5. Si vous ne pouvez pas vérifier la signature numérique, cliquez sur Exécuter pour démarrer l'installation.
6. Dans la fenêtre Installation de tiers, cliquez sur Suivant.
7. Acceptez le contrat de licence et cliquez sur Suivant.
8. Spécifiez le répertoire de destination pour installer le noeud d'orchestrateur, puis cliquez sur Suivant.

   Le programme d'installation crée le dossier automatiquement s'il n'existe pas.
9. Dans la fenêtre Conditions préalables à l'installation de CA Process Automation, cliquez sur Suivant.

   L'une des fenêtres suivantes inclut la case à cocher suivante :

   Utiliser un domaine

   Spécifie si ce noeud de cluster est associé à l'orchestrateur de domaine

   Option désactivée : ce noeud de cluster n'est pas associé à l'orchestrateur de domaine.

   Dans la fenêtre de confirmation, cliquez sur Suivant.
10. Pour passer au programme d'installation de CA Process Automation, cliquez sur Terminer.
11. Dans la fenêtre de bienvenue, cliquez sur Suivant.

12. Acceptez le contrat de licence et cliquez sur Suivant.
13. Spécifiez le répertoire de base Java. Le programme d'installation de CA Process Automation pré-remplit ce champ avec le dernier JDK approprié localisé dans le chemin d'accès. Si nécessaire, accédez au répertoire dans lequel le JDK est installé et cliquez sur Suivant.

    Le kit de développement Java est validé et l'installation de l'orchestrateur commence. La copie des fichiers prend environ une minute.
14. Renseignez la fenêtre Configuration, puis cliquez sur Suivant.

    orchestrateur

    Spécifie l'orchestrateur auquel le noeud de cluster doit être ajouté. L'orchestrateur sélectionné dans la liste déroulante doit être configuré avec un nom d'hôte public indiquant le nom de domaine complet du serveur sur lequel l'équilibreur de charge est installé.

    Noeud de travail de l'équilibreur de charge

    Spécifie le nom de noeud, par exemple, node2. Le nom de ce noeud est indiqué dans le fichier workers.properties d'Apache, où *hostname* correspond au nom de l'hôte sur lequel vous installez le noeud de cluster :

    worker.**node2**.host=*hostname*.*mycompany*.com

    Remarque : La première installation de l'orchestrateur de domaine est node1. Pour le deuxième noeud, saisissez **node2.**
15. Affichez le nom de société et cliquez sur Suivant.
16. Saisissez le même mot de passe de certificat saisi lors de l'installation de l'orchestrateur de domaine, puis cliquez sur Suivant.

    Si vous perdez ou oubliez ce mot de passe de certificat, vous devrez réinstaller tous les orchestrateurs dans le système, en commençant par l'orchestrateur de domaine.
17. Spécifiez un dossier du menu Démarrer et cliquez sur Suivant.
18. Entrez les propriétés générales de l'orchestrateur et cliquez sur Suivant.

    Pour plus d'informations sur chaque propriété, consultez la section Installer et configurer l'orchestrateur de domaine.
19. Affichez les paramètres de sécurité, puis cliquez sur Suivant.
20. Affichez les paramètres de la base de données, puis cliquez sur Suivant.
21. Affichez les paramètres de la base de données de reporting et cliquez sur Suivant pour terminer l'installation.
22. Cliquez sur Terminer.

    Le noeud de cluster de l'orchestrateur sélectionné est installé.

Synchronisation horaire d'un noeud de cluster

Tous les noeuds de cluster d'un orchestrateur doivent marquer le même temps horloge, synchronisé avec un serveur de synchronisation externe standard. Utilisez l'une des approches suivantes pour synchroniser l'heure de tous les noeuds d'un cluster :

- Synchronisez tous les orchestrateurs et les noeuds de cluster vers un serveur de synchronisation externe standard (procédure préférée).
- Synchronisez manuellement l'heure de tous les noeuds de cluster supplémentaires, comme suit :
  1. Vérifiez l'exactitude de l'heure de tous les noeuds de cluster.
  2. Exécutez la commande de système d'exploitation appropriée sur chaque noeud de cluster pour synchroniser l'heure de l'ensemble des noeuds de cluster.

Chapitre 12: Réglage de CA Process Automation

Ce chapitre traite des sujets suivants :

Amélioration des performances de CA Process Automation (page 216)

Amélioration des performances de CA Process Automation

Lorsque vous souhaitez renforcer ou améliorer les performances, tenez compte des directives suivantes :

- Convertissez chaque orchestrateur autonome en cluster.

  L'ajout d'un deuxième noeud peut améliorer les performances jusqu'à 80 %. L'amélioration réalisée dépend de nombreuses variables, y compris le contenu CA Process Automation en cours d'exécution.

- Contenu
  - Ensembles de données globaux

    Limitez les références aux ensembles de données globaux, car leur accès est sérialisé. En d'autres termes, un seul objet à la fois peut accéder à un ensemble de données. Cette directive s'applique à l'accès en écriture (non en lecture).

    Il est conseillé d'effectuer une copie de niveau processus des données requises, puis de consulter cet ensemble de données de processus.

  - Processus en ligne

    Limitez l'utilisation de lancement de processus en ligne aux situations remplissant les conditions suivantes :

    - Le processus en ligne compte moins de 10 opérateurs.
    - Le processus en ligne n'est pas appelé dans une boucle.

- UC
  - Surveillez l'utilisation des UC sur tous les noeuds d'orchestrateur pour déterminer ceux qui peuvent tirer meilleur parti des unités centrales ou des noyaux supplémentaires.
  - Ajoutez plusieurs unités centrales ou noyaux si nécessaire.
  - Lors de l'exécution dans un environnement virtuel, dédiez les unités centrales aux ordinateurs virtuels CA Process Automation.

- Mémoire
  - Lors de l'exécution dans un environnement virtuel, dédiez la mémoire RAM aux ordinateurs virtuels CA Process Automation.
  - Surveillez l'utilisation de la mémoire par les processus sur tous les noeuds d'orchestrateur pour déterminer si de la mémoire RAM supplémentaire est requise.

- Optimisation du serveur de l'ordinateur virtuel

  Consultez votre fournisseur de serveur l'ordinateur virtuel pour obtenir des instructions sur le renforcement des performances.

- Optimisation et maintenance de la base de données

Consultez votre fournisseur de serveur de base de données pour obtenir des instructions sur la procédure à suivre pour renforcer et maintenir les performances de la base de données CA Process Automation. Ces instructions incluent généralement la réindexation de la base de données, la mise à jour des statistiques, ainsi que la surveillance et la maintenance du système de fichiers sur lequel les données sont stockées.

- Désactivation de l'ensemble des fonctionnalités non requises
  - Catalyst

    Si vous n'utilisez pas de connecteurs Catalyst, recherchez la valeur suivante dans le fichier OasisConfig.properties et définissez sur false :

    ```
    # enable connector
    ucf.connector.enabled=true
    ```

  - Génération de rapports

    Si vous n'utilisez pas le reporting, insérez la paire valeur/clé suivante dans le fichier OasisConfig.properties. Les changements apportés à ce fichier s'appliqueront lors du redémarrage du service CA Process Automation.

    ```
    oasis.disable.reporting.manager=true
    ```

- VMware

  Si vous utilisez VMware, modifiez le contrôleur virtuel de l'interface réseau de E1000 à VMXNET3. En règle générale, ce changement améliore les performances et la fiabilité.

Annexe A: Utilisation de CA SiteMinder avec CA Process Automation

CA SiteMinder fournit des fonctionnalités d'authentification unique via des domaines de cookie unique et multiple, permettant ainsi aux utilisateurs d'accéder à des applications sur plusieurs serveurs et plates-formes Web, en entrant leurs informations d'identification une seule fois pour chaque session.

Ce chapitre traite des sujets suivants :

Conditions requises pour CA SiteMinder (page 220)
Configuration des objets de serveur de politiques CA SiteMinder (page 220)
Intégrez CA Process Automation avec IIS pour l'authentification unique (page 222)
Configuration de l'hôte IIS pour la redirection des demandes vers Tomcat (page 223)
Intégrer CA Process Automation avec Apache pour l'authentification unique (page 225)
Activer la déconnexion dans CA Process Automation pour l'authentification unique (page 226)

Conditions requises pour CA SiteMinder

Vérifiez que votre système remplit les conditions préalables suivantes pour l'installation de CA Process Automation avec CA SiteMinder :

- Un serveur CA EEM intégré au même LDAP/AD utilisé comme annuaire d'utilisateurs dans le serveur de politiques CA SiteMinder.
- Un agent Web CA SiteMinder intégré avec IIS ou Apache.

Vous pouvez utiliser l'agent Apache de SiteMinder uniquement lorsque vous disposez d'un équilibreur de charge basé sur Apache et d'un orchestrateur mis en cluster. Dans le cas d'un orchestrateur autonome, définissez le transfert de port du port Tomcat 8080 au port IIS 80 pour que l'agent IIS SM fonctionne.

Remarque : Pour plus d'informations, consultez le *Manuel d'installation de l'agent Web CA SiteMinder*.

A des fins de sécurité, collaborez directement avec votre administrateur CA SiteMinder pour vous assurer de bien comprendre et suivre toutes les directives existantes pour l'utilisation de CA SiteMinder au sein de votre entreprise.

Important : Vous devez réinstaller les agents CA Process Automation au lieu de simplement redémarrer, lorsque l'URL de l'orchestrateur de domaine est modifiée. Les modifications suivantes peuvent affecter l'URL de l'orchestrateur de domaine :

- Modification de l'orchestrateur de domaine du mode SSO-enabled (authentification unique activée) au mode SSO-disabled (authentification unique désactivée)
- Modification de l'orchestrateur de domaine du mode SSO-disabled au mode SSO-enabled
- Pointage de l'orchestrateur de domaine vers un serveur CA SSO différent.

Configuration des objets de serveur de politiques CA SiteMinder

Pour configurer CA SiteMinder, accédez à l'interface d'administration du serveur de politiques CA SiteMinder. Pour plus d'informations, consultez le *Manuel de configuration du serveur de politiques CA SiteMinder*.

Important : Avant de configurer CA SiteMinder pour CA Process Automation, consultez votre administrateur CA SiteMinder. Votre société a pu établir des politiques de sélection ou de création de domaines, des conventions d'attribution de nom pour d'autres entités ou d'autres mesures de sécurité par site.

Pour configurer un objet d'agent Web à intégrer à CA Process Automation :

1. Créez un objet de configuration d'agent dans la section d'infrastructure de l'interface d'administration de CA SiteMinder. Sélectionnez ApacheDefaultSettings ou IISDefaultSettings, selon l'agent Web que doivent héberger les serveurs.
   - Accédez à la propriété BadUrlChars de l'agent Web et supprimez les parties /. et // de la propriété.
   - Accédez à la propriété IgnoreExt et supprimez la partie .gif,.jpg,.jpeg,.png de la valeur de la propriété.
   - Accédez à la propriété LogoffUri et définissez-la à "/itpam/Logout".
2. Créez un objet de configuration d'hôte. Sélectionnez ApacheDefaultSettings ou IISDefaultSettings, selon l'agent Web que doivent héberger les serveurs.
3. Créez un objet d'annuaire dans la section d'infrastructure de l'interface d'administration de CA SiteMinder.
4. Créez ou sélectionnez un domaine dans la section de domaine de l'interface administrateur de CA SiteMinder.
5. Créez un domaine dans la section de domaine de l'interface utilisateur du serveur de politiques SiteMinder CA.
6. Dans le nouveau domaine, spécifiez le nom d'agent correct, définissez le filtre de ressource sur /itpam, puis sélectionnez Protected (protégé) dans la section de protection des ressources par défaut.
7. Dans le nouveau domaine, créez une règle avec une ressource * afin que la ressource ait l'aspect web_agent/itpam*, puis sélectionnez tous les éléments de la section d'actions.

   Remarque : Pour spécifier cette règle dans la section des politiques, ajoutez-la à une politique existante ou à une nouvelle politique. Pour plus d'informations, consultez le *Manuel de configuration du serveur de politiques CA SiteMinder*.
8. Créez un sous-domaine pour chacune des URL suivantes et sélectionnez Unprotected (non protégé) dans la section de protection des ressources par défaut :
   - /swaref.xsd
   - /genericNoSecurity
   - /images
   - /StartAgent
   - /itpamclient
   - /ServerConfigurationRequestServlet
   - /MirroringRequestProcessor
   - /soapAttachment
   - /AgentConfigurationRequestServlet

- /soap
- /css
- /js

9. Créez une politique dans la section des politiques, puis ajoutez la règle créée à l'étape 7 dans la politique.

   Pour plus d'informations, consultez le *Manuel de configuration du serveur de politiques CA SiteMinder*.

10. (Facultatif) Utilisez les valeurs par défaut pour créer une variable de réponse personnalisée et utilisez-la comme paramètre d'authentification unique.

    a. Créez un attribut de réponse personnalisé **pamuser** de type WebAgent-HTTP-Header-Variable.

    b. Définissez la valeur de la variable comme paramètre utilisé pour l'ID d'utilisateur LDAP/ActiveDirectory.

    c. Ajoutez cette réponse personnalisée à la règle mentionnée à l'étape 9.

       Remarque : Lors de l'installation de CA Process Automation, spécifiez le paramètre d'en-tête **pamuser** comme paramètre d'authentification unique avec le type d'authentification unique comme **en-tête**. Pour plus d'informations, consultez le *Manuel de configuration du serveur de politiques CA SiteMinder*.

Intégrez CA Process Automation avec IIS pour l'authentification unique

Remarque : Pour intégrer CA SiteMinder avec une mise en cluster, sélectionnez l'agent Apache SiteMinder.

Pour configurer l'authentification unique avec IIS

1. Faites en sorte que votre administrateur CA SiteMinder installe l'agent Web CA SiteMinder sur un ordinateur sur lequel IIS est installé.
2. Si IIS est configuré pour SSL, décompressez IIS_https_httpfolders.zip, situé dans le dossier /SSO/IIS du média des programmes tiers requis pour CA Process Automation, dans le répertoire de base du site Web sur lequel CA SiteMinder est intégré.

3. Vérifiez si les dossiers suivants sont créés dans le répertoire de base :
   - c2orepository +
   - itpam
   - mirroringrepository
4. Ouvrez le gestionnaire IIS et supprimez le mode SSL des dossiers suivants :

   Sur le site Web :

   - c2orepository
   - mirroringrepository

   Dans le dossier itpam :

   - MirroringRequestProcessor
   - StartAgent
   - genericNoSecurity

   Pour supprimer le mode SSL :

   a. Ouvrez les propriétés du dossier correspondant.

   b. Sélectionnez l'onglet Sécurité de répertoire, puis cliquez sur Modifier dans la section Communication sécurisée et décochez la case Requérir un canal sécurisé (SSL).

   Remarque : Pour intégrer CA Process Automation, utilisez le filtre de redirection de Tomcat lorsque l'agent Web CA SiteMinder est déployé sur IIS.

Configuration de l'hôte IIS pour la redirection des demandes vers Tomcat

Elément requis

L'agent CA SiteMinder doit être exécuté sur le même serveur IIS, avant de configurer le redirecteur Tomcat pour la redirection des demandes vers CA Process Automation. Pour plus d'informations, consultez le *Manuel d'installation de CA SiteMinder*.

Procédez comme suit :

1. Vérifiez que le serveur Web IIS est installé et en cours d'exécution.
2. Copiez le dossier TomcatRedirector sur l'ordinateur sur lequel l'hôte IIS est installé, de préférence dans le chemin d'accès suivant :

   ```
   C:\Program Files\CA\SharedComponents
   ```

3. Modifiez le fichier isapi_redirect.properties dans le dossier bin afin qu'il reflète le chemin d'accès approprié, le cas échéant.

   Exemple :

   ```
   # Configuration file for the Jakarta ISAPI Redirector
   # The path to the ISAPI Redirector Extension, relative to the
   website
   # This must be in a virtual directory with execute privileges.
   extension_uri=/TomcatRedirector/isapi_redirect.dll
   ```

   Remarque : TomcatRedirector est le nom de répertoire virtuel.

   ```
   # Full path to the log file for the ISAPI Redirector
   log_file=C:\Program
   Files\CA\SharedComponents\TomcatRedirector\logs\isapi_redirect.
   log
   # Log level (debug, info, warn, error or trace)
   log_level=error
   # Full path to the workers.properties file
   worker_file=c:\Program
   Files\CA\SharedComponents\TomcatRedirector\conf\workers.propert
   ies
   # Full path to the uriworkermap.properties file\
   worker_mount_file=c:\Program
   Files\CA\SharedComponents\TomcatRedirector\conf\uriworkermap.pr
   operties
   ```

4. Modifiez le nom d'hôte du fichier TomcatRedirector\conf\workers.properties afin qu'il reflète le nom d'hôte approprié. Remplacez les références à localhost.

   Exemple :

   ```
   # statement and uncomment the three worker.ajp13w01 lines
   ##############################################################
   #######
   # The workers that jk should create and work with
   worker.list=ajp13w01
   # Defining a worker named ajp13w01 and of type ajp13
   # Note that the name and the type do not have to match.
   worker.ajp13w01.type=ajp13
   worker.ajp13w01.host=pa-w2k3
   worker.ajp13w01.port=8009
   ```

   Remarque : Dans le code précédent, pa-w2k3 est l'ordinateur sur lequel CA Process Automation est installé.

5. Ouvrez la console de gestionnaire IIS.

6. Cliquez avec le bouton droit de la souris sur le site Web par défaut et sélectionnez un nouveau répertoire virtuel et indiquez le dossier TomcatRedirector\bin que vous avez créé à l'étape 4.

7. Accédez au dossier TomcatRedirector\logs de l'explorateur Windows et octroyez toutes les autorisations d'accès au fichier journal de ce dossier à l'utilisateur du service réseau.
8. Cliquez avec le bouton droit de la souris sur le répertoire virtuel et sélectionnez les propriétés. Cliquez ensuite sur l'option Créer qui se trouve à côté du nom de l'application, sélectionnez Scripts et exécutables pour les autorisations Exécuter, et cliquez sur OK.

   Remarque : Vérifiez que la valeur du champ Nom de l'application correspond au nom de répertoire virtuel fourni dans le fichier isapi_redirect.properties (étape 3).

   a. Cliquez avec le bouton droit de la souris sur Extensions du service Web, attribuez-lui le nom TomcatRedirector et sélectionnez le chemin d'accès au fichier TomcatRedirector\bin\isapi_redirect.dll auquel vous souhaitez ajouter une extension de service Web. Sélectionnez Définir l'état de l'extension à Autorisée.

   b. Recyclage du service d'administration IIS
9. Ajoutez le fichier isapi_redirect.dll comme filtre ISAPI dans votre site Web IIS. Ouvrez le gestionnaire IIS et cliquez avec le bouton droit de la souris sur le dossier Sites Web pour ouvrir la boîte de dialogue de propriétés pour tous les sites Web, sélectionnez l'onglet de filtre ISAPI, cliquez sur Ajouter et sélectionnez le fichier isapi_redirect.dll en tant qu'exécutable.
10. Vérifiez que les demandes sont envoyées vers Tomcat en saisissant http://localhost:80.

Intégrer CA Process Automation avec Apache pour l'authentification unique

Pour configurer l'authentification unique avec Apache

1. Faites en sorte que votre administrateur CA SiteMinder installe l'agent Web CA SiteMinder sur un ordinateur sur lequel Apache est installé.
2. Configurez Apache avec les paramètres d'hôte public. Pour plus d'informations, consultez la section Installation de l'orchestrateur de domaine (page 96).

   Remarque : Contactez votre administrateur CA SiteMinder pour plus d'informations.

Activer la déconnexion dans CA Process Automation pour l'authentification unique

Vous pouvez autoriser la déconnexion de l'authentification unique dans CA Process Automation.

Procédez comme suit :

1. Accédez à l'emplacement suivant :

   répertoire_installation/server/c2o/.config

2. Double-cliquez pour ouvrir le fichier OasisConfig.properties.
3. Modifiez ALLOW_SSO_LOGOUT sur True.

Annexe B: Ports utilisés par CA Process Automation

Cette annexe contient les tableaux qui décrivent en détail l'utilisation des ports par les composants CA Process Automation. Ces tableaux contiennent toutes les informations relatives à chaque composant, y compris des informations en doubles à des fins de clarté.

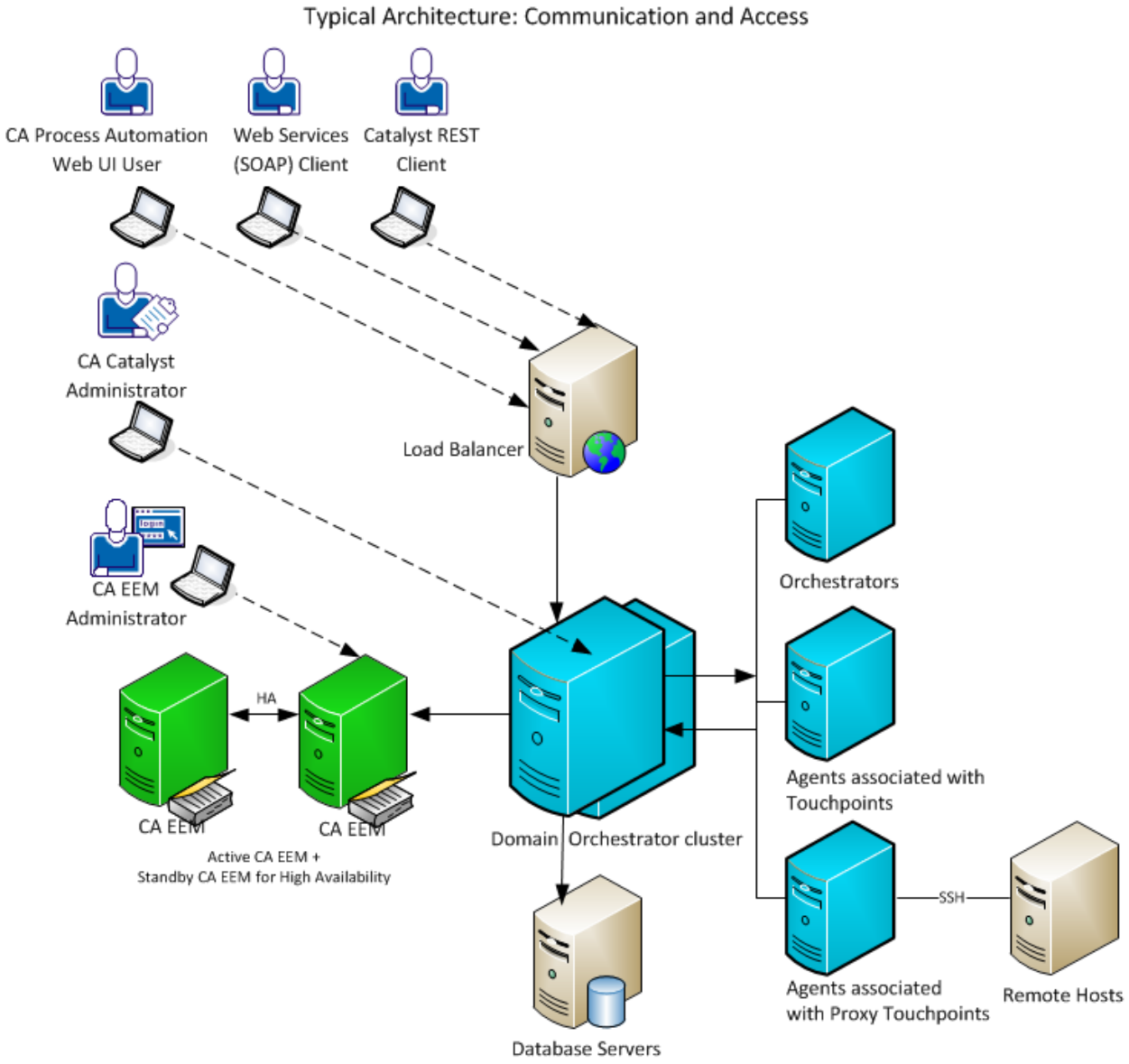
Pour en savoir plus sur les communications des composants, consultez la rubrique Communications dans une architecture standard (page 228).

Ce chapitre traite des sujets suivants :

Communications dans une architecture standard (page 228)
Ports utilisés par CA EEM (page 229)
Ports utilisés par l'équilibreur de charge (page 231)
Ports utilisés par un orchestrateur (page 234)
Ports utilisés par un agent (page 242)
Ports utilisés par les serveurs de base de données (page 244)
Ports utilisés par les clients Web (page 245)

Communications dans une architecture standard

Le schéma suivant illustre les relations entre des composants référencés dans cette annexe sur les ports utilisés par CA Process Automation.



Informations complémentaires :

Détermination de l'emplacement des composants pris en charge (page 67)

Ports utilisés par CA EEM

Les tableaux suivants récapitulent les ports utilisés pour les communications de CA Embedded Entitlements Manager (CA EEM).

Communications à partir de CA EEM

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
CA EEM	Tout	CA EEM	509	TCP	Configuration de CA EEM	Utilisé par CA EEM iTechPoz lorsque CA EEM est configuré en tant que cluster de haute disponibilité.
CA EEM	Any	CA EEM	1684	TCP	Configuration de CA EEM	Utilisé par le routeur CA EEM iTechPoz lorsque CA EEM est configuré en tant que cluster de haute disponibilité (CA EEM 8.4 uniquement)
CA EEM	Any	CA EEM	5250	TCP	Configuration de CA EEM	Utilisé par CA EEM iGateway lorsque CA EEM est configuré en tant que cluster de haute disponibilité.

Communications vers CA EEM

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
CA EEM	Any	CA EEM	509	TCP	Configuration de CA EEM	Utilisé par CA EEM iTechPoz lorsque CA EEM est configuré en tant que cluster de haute disponibilité.

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
CA EEM	Any	CA EEM	1684	TCP	Configuration de CA EEM	Utilisé par le routeur CA EEM iTechPoz lorsque CA EEM est configuré en tant que cluster de haute disponibilité (CA EEM 8.4 uniquement)
CA EEM	Any	CA EEM	5250	TCP	Configuration de CA EEM	Utilisé par CA EEM iGateway lorsque CA EEM est configuré en tant que cluster de haute disponibilité.
orchestrateur	Any	CA EEM	5250	TCP	Configuration de CA EEM	Utilisés par CA EEM iGateway
Navigateur Web (administrateur CA EEM)	Any	CA EEM	5250	TCP	Configuration de CA EEM	Navigateur Web avec accès à l'interface utilisateur CA EEM.

Ports utilisés par l'équilibreur de charge

Les tableaux suivants récapitulent les ports utilisés pour les communications de l'équilibreur de charge configuré. Les équilibreurs de charge pris en charge incluent NGINX, Apache et F5. Les ports incluent les ports de Jboss@Orchestrator et Jetty@Orchestrator.

Communications à partir de l'équilibreur de charge

Remarque : Vous pouvez configurer des ports d'écoute pour un équilibreur de charge dans le fichier indiqué dans la colonne Configuration. La documentation de chaque équilibreur de charge contient l'emplacement de chaque fichier de configuration.

Apache

httpd.conf

tomcat.connector.ajp.port

NGINX

pam-server.conf

secure-pam-server.conf

pam-rest.conf

F5

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
Equilibreur de charge	Tout	orchestrateur	80	HTTP	httpd.conf	L'équilibreur de charge communique avec les orchestrateurs sur ce port. Ce port ne s'applique pas à NGINX.

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
Equilibreur de charge	Tout	orchestrateur	443	HTTPS	httpd.conf	L'équilibreur de charge communique avec les orchestrateurs sécurisés sur ce port. Ce port ne s'applique pas à NGINX.
Equilibreur de charge	Tout	orchestrateur	8010	TCP/AJP	tomcat.connector.ajp.port	Loadbalancer - port du connecteur AJP entre l'équilibreur de charge et l'orchestrateur. Ce port ne s'applique pas à NGINX.
Equilibreur de charge	Tout	orchestrateur	8080	HTTP	httpd.conf, pam-server.conf	L'équilibreur de charge communique avec les orchestrateurs sur ce port.
Equilibreur de charge	Tout	orchestrateur	8443	HTTPS	httpd.conf, secure-pam-server.conf	L'équilibreur de charge communique avec les orchestrateurs sécurisés sur ce port.
Equilibreur de charge	Tout	orchestrateur	8009	TCP/AJP	tomcat.connector.ajp.port	Loadbalancer - port du connecteur AJP entre l'équilibreur de charge et l'orchestrateur. Ce port ne s'applique pas à NGINX.
Equilibreur de charge	Tout	orchestrateur	7000	HTTP	node0-config.xml, http.port, pam-rest.conf	Port du conteneur Catalyst de CA Process Automation
Equilibreur de charge	Tout	orchestrateur	7443	HTTPS	node0-config.xml, https.port, pam-rest.conf	Port sécurisé du conteneur Catalyst de CA Process Automation

Communications vers l'équilibreur de charge

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
Client Catalyst REST	Tout	Equilibreur de charge	7000	HTTP	node0-config.xml, http.port, pam-rest.conf	Port du conteneur Catalyst de CA Process Automation
Client Catalyst REST	Tout	Equilibreur de charge	7443	HTTPS	node0-config.xml, https.port, pam-rest.conf	Port sécurisé du conteneur Catalyst de CA Process Automation
Agent	Tout	Equilibreur de charge	80	HTTP	httpd.conf	Port de l'équilibreur de charge pour les communications de base
Agent	Tout	Equilibreur de charge	443	HTTPS	httpd.conf	Port de l'équilibreur de charge pour les communications sécurisées
Navigateur Web (utilisateur CA Process Automation)	Tout	Equilibreur de charge	80	TCP	httpd.conf	Port de l'équilibreur de charge pour les communications de base
Navigateur Web (utilisateur CA Process Automation)	Tout	Equilibreur de charge	443	TCP	httpd.conf	Port de l'équilibreur de charge pour les communications sécurisées
Client de service Web (SOAP)	Tout	Equilibreur de charge	80	TCP	httpd.conf	Port de l'équilibreur de charge pour les communications de base
Client de service Web (SOAP)	Tout	Equilibreur de charge	443	TCP	httpd.conf	Port de l'équilibreur de charge pour les communications sécurisées

Ports utilisés par un orchestrateur

Les tableaux suivants récapitulent les ports utilisés pour les communications, notamment :

- Pour les communications d'un orchestrateur vers un autre composant dans un système CA Process Automation
- Pour les communications entre les orchestrateurs
- Pour les communications vers un orchestrateur à partir d'un autre composant dans un système CA Process Automation

Pour les communications d'un orchestrateur vers un autre composant

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
orchestrateur	Tout	CA EEM	5250	TCP	Configuration de CA EEM	Utilisés par CA EEM iGateway
orchestrateur	Tout	Agent	7003	HTTP/HTTPS	Script d'installation d'agent	**Désapprouvé** L'agent écoute les communications sur ce port lorsque l'ancienne méthode de communication avec les orchestrateurs est utilisée.
orchestrateur	Tout	Microsoft SQL Database Server	1433	TCP	Microsoft SQL Server configuré	Vous pouvez changer le port de base de données dans l'installation de serveur de base de données. Sa valeur par défaut est 1433.
orchestrateur	Tout	Serveur de base de données MySQL	3306	TCP	MySQL configuré	Vous pouvez changer le port de base de données dans l'installation de serveur de base de données. Sa valeur par défaut est 3306.

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
orchestrateur	Tout	serveur de base de données Oracle	1521	TCP	Ecouteur Oracle configuré	Vous pouvez changer le port de base de données lors de la création de l'écouteur. La valeur par défaut du port d'écoute Oracle est 1521. Vous pouvez associer l'instance de base de données à un écouteur différent. Reportez-vous à la configuration Oracle.
orchestrateur	Tout	Hôte distant cible	22	TCP	Port SSH standard	Utilisé pour les communications SSH avec un point de contact de proxy ou un groupe d'hôtes.

Communication entre des orchestrateurs de domaine et d'autres types d'orchestrateurs

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
orchestrateur de domaine	Tout	Autre type d'orchestrateur	1090	TCP	jboss.remoting.port	Le port JBoss Remoting est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	1098	TCP	jboss.rmi.port	Le port JBoss RMI est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	1099	TCP	jboss.jndi.port	Le port JBoss JNDI est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	1100	TCP	jboss.ha.jndi.port	Le port JBoss HA_Java Namming and Directory Interface est utilisé uniquement entre les orchestrateurs.

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
orchestrateur	Tout	Autre type d'orchestrateur	1101	TCP	jboss.ha.jndi.port	Le port JBoss HA-Java Remote Method Invocation est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	1102	UDP	jboss.mcast.jndi.autodiscovery.port	Le port JBoss JNDI Autodiscovery est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	3873	TCP	jboss.remoting.transport.Connector.port	Le port JBoss EJB3 Remoting Connector est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	4444	TCP	jboss.rmi.object.port	Le port JBoss RMI Server est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	4445	TCP	jboss.ha.pooledinvoker.serverbind.port	Le port JBoss Pooled Invoker est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	4446	TCP	jboss.pooledinvoker.serverbind.port	Le port JBoss HA Pooled Invoker est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	4447	TCP	jboss.ha.rmi.object.port	Le port JBoss HA-RMI Server est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	4448	TCP		Le port JBoss HA Pooled Invoker est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	4457	TCP	jboss.service.binding.port	Le port JBoss Messaging est utilisé uniquement entre les orchestrateurs.

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
orchestrateur	Tout	Autre type d'orchestrateur	4712	TCP	jboss.tx.recovery.manager.port	Le port JBoss Transaction Status Recovery Manager est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	4713	TCP		Le port JBoss Transaction Status Manager est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	7001	HTTP/HTTPS	oasis.jxta.port	Port utilisé pour les communications entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	7600	TCP	jboss.jgroups.tcp.tcp_port	Le port JBoss de mise en cluster est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	7900	TCP	jboss.messaging.datachanneltcpport	Le port JBoss de mise en cluster est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	7901	TCP	jboss.messaging.controlchanneltcpport	Le port JBoss de mise en cluster est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	8083	TCP	jboss.rmi.classloader.webservice.port	Le port JBoss RMI WebService est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	Autre type d'orchestrateur	8080			
orchestrateur	Tout	Autre type d'orchestrateur	8443			
orchestrateur	Tout	Autre type d'orchestrateur				

Communication entre des noeuds d'orchestrateur mis en cluster

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
orchestrateur	Tout	orchestrateur	1090	TCP	jboss.remoting.port	Le port JBoss Remoting est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	1098	TCP	jboss.rmi.port	Le port JBoss RMI est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	1099	TCP	jboss.jndi.port	Le port JBoss JNDI est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	1100	TCP	jboss.ha.jndi.port	Le port JBoss HA_Java Namming and Directory Interface est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	1101	TCP	jboss.ha.jndi.port	Le port JBoss HA-Java Remote Method Invocation est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	1102	UDP	jboss.mcast.jndi.autodiscovery.port	Le port JBoss JNDI Autodiscovery est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	3873	TCP	jboss.remoting.transport.Connector.port	Le port JBoss EJB3 Remoting Connector est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	4444	TCP	jboss.rmi.object.port	Le port JBoss RMI Server est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	4445	TCP	jboss.ha.pooledinvoker.serverbind.port	Le port JBoss Pooled Invoker est utilisé uniquement entre les orchestrateurs.

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
orchestrateur	Tout	orchestrateur	4446	TCP	jboss.pooledinvoker.serverbind.port	Le port JBoss HA Pooled Invoker est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	4447	TCP	jboss.ha.rmi.object.port	Le port JBoss HA-RMI Server est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	4448	TCP		Le port JBoss HA Pooled Invoker est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	4457	TCP	jboss.service.binding.port	Le port JBoss Messaging est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	4712	TCP	jboss.tx.recovery.manager.port	Le port JBoss Transaction Status Recovery Manager est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	4713	TCP		Le port JBoss Transaction Status Manager est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	7001	HTTP/HTTPS	oasis.jxta.port	Port utilisé pour les communications entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	7600	TCP	jboss.jgroups.tcp.tcp_port	Le port JBoss de mise en cluster est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	7900	TCP	jboss.messaging.datachanneltcpport	Le port JBoss de mise en cluster est utilisé uniquement entre les orchestrateurs.

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
orchestrateur	Tout	orchestrateur	7901	TCP	jboss.messaging.controlchanneltcpport	Le port JBoss de mise en cluster est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	8083	TCP	jboss.rmi.classloader.webservice.port	Le port JBoss RMI WebService est utilisé uniquement entre les orchestrateurs.
orchestrateur	Tout	orchestrateur	61618			ActiveMQ...

Remarque : CA Process Automation utilise JBoss 5.1. JBoss 5.1 utilise des ports dynamiques intermittents compris dans la plage 49152-65535 lorsqu'il est configuré en tant que cluster pour les communications entre les noeuds (orchestrateurs uniquement). Notez que la plupart des ports sont utilisés à des fins de gestion interne de cluster. Il n'est pas recommander de répartir les clusters par liens WAN//pare-feu. La configuration en cluster par défaut utilise la multidiffusion et si les communications en multidiffusion ne sont pas ouvertes de bout en bout entre les noeuds du cluster, elles ne font pas parties du même cluster et peuvent donner lieu à un comportement erratique.

Communications vers un orchestrateur mis en cluster à partir d'un autre composant

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
Equilibreur de charge	Tout	orchestrateur	8080	HTTP	Apache httpd.conf	L'équilibreur de charge Apache communique avec les orchestrateurs sur ce port.
Equilibreur de charge	Tout	orchestrateur	8443	HTTPS	Apache httpd.conf	L'équilibreur de charge Apache communique avec les orchestrateurs sécurisés sur ce port.
Equilibreur de charge	Tout	orchestrateur	7000	HTTP	node0-config.xml, http.port	Port du conteneur Catalyst de CA Process Automation

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
Equilibreur de charge	Tout	orchestrateur	7443	HTTPS	node0-config.xml, https.port	Port sécurisé du conteneur Catalyst de CA Process Automation
Equilibreur de charge	Tout	orchestrateur	8009	TCP/AJP	tomcat.connector.ajp.port	Loadbalancer - Port du connecteur AJP entre l'équilibreur de charge et l'orchestrateur
Agent	Tout	orchestrateur	8080	HTTP	tomcat.connector.http.port	Communications désapprouvées uniquement
Agent	Tout	orchestrateur	8443	HTTPS	tomcat.secure.port	Communications désapprouvées uniquement
Agent	Tout	orchestrateur	7001	HTTP/HTTPS	oasis.jxta.port	Port désapprouvé

Communications vers un orchestrateur non mis en cluster à partir d'un autre composant

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
Agent	Tout	orchestrateur	8080	HTTP	tomcat.connector.http.port	Interface utilisateur CA Process Automation : port de base

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
Agent	Tout	orchestrateur	8443	HTTPS	tomcat.secure.port	Interface utilisateur CA Process Automation : port sécurisé
Agent	Tout	orchestrateur	7001	HTTP/HTTPS	oasis.jxta.port	Port désapprouvé
orchestrateur	Tout	Agent	80	HTTP	Jetty	Connexion de socket Web établie par les agents
orchestrateur	Tout	Agent	443	HTTPS	Jetty	Connexion de socket Web établie par les agents

Ports utilisés par un agent

Les tableaux suivants récapitulent les ports utilisés pour les communications d'un agent CA Process Automation.

Communications à partir d'un agent

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
Agent	Tout	orchestrateur	8080	HTTP	tomcat.connector.http.port	Interface utilisateur CA Process Automation : port pour les communications de base
Agent	Tout	orchestrateur	8443	HTTPS	tomcat.secure.port	Interface utilisateur CA Process Automation : port pour les communications sécurisées
Agent	Tout	Equilibreur de charge Apache	80	HTTP	Apache httpd.conf	Port de l'équilibreur de charge Apache pour les communications de base

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
Agent	Tout	Equilibreur de charge Apache	443	HTTPS	Apache httpd.conf	Port de l'équilibreur de charge Apache pour les communications sécurisées
Agent	Tout	orchestrateur	7001	HTTP/HTTPS	oasis.jxta.port	Port de serveur désapprouvé
Agent	Tout	orchestrateur	80	HTTP	Jetty	Port du serveur
Agent	Tout	orchestrateur	443	HTTPS	Jetty	Port du serveur
Agent	Tout	Hôte distant cible	22	TCP	Port SSH standard	Utilisé pour les communications SSH avec un point de contact de proxy ou un groupe d'hôtes

Communications vers un agent

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
orchestrateur	Tout	Agent	7003	HTTP/HTTPS	Script d'installation d'agent	L'agent écoutait auparavant les communications avec les orchestrateurs sur ce port désapprouvé.
orchestrateur	Tout	Agent	80	HTTP	Jetty	Connexion de socket Web établie par les agents
orchestrateur	Tout	Agent	443	HTTPS	Jetty	Connexion de socket Web établie par les agents

Ports utilisés par les serveurs de base de données

Le tableau suivant récapitule les ports utilisés pour les communications d'un serveur de base de données.

Communications vers un serveur de base de données

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
orchestrateur	Tout	Microsoft SQL Database Server	1433	TCP	Microsoft SQL Server configuré	Vous pouvez changer le port de base de données dans l'installation de serveur de base de données. Sa valeur par défaut est 1433.
orchestrateur	Tout	Serveur de base de données MySQL	3306	TCP	MySQL configuré	Vous pouvez changer le port de base de données dans l'installation de serveur de base de données. Sa valeur par défaut est 3306.
orchestrateur	Tout	serveur de base de données Oracle	1521	TCP	Ecouteur Oracle configuré	Vous pouvez changer le port de base de données lors de la création de l'écouteur. La valeur par défaut du port d'écoute Oracle est 1521. Vous pouvez associer l'instance de base de données à un écouteur différent. Reportez-vous à la configuration Oracle.

Ports utilisés par les clients Web

Le tableau suivant récapitule les ports utilisés pour les communications à partir des clients Web.

Communications à partir des clients Web

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
Navigateur Web (administrateur CA EEM)	Any	CA EEM	5250	TCP	Configuration de CA EEM	Navigateur Web avec accès à l'interface utilisateur CA EEM.
Navigateur Web (utilisateur CA Process Automation)	Any	Equilibreur de charge Apache	80	TCP	Apache httpd.conf	Port de l'équilibreur de charge Apache pour les communications de base
Navigateur Web (utilisateur CA Process Automation)	Any	Equilibreur de charge Apache	443	TCP	Apache httpd.conf	Port de l'équilibreur de charge Apache pour les communications sécurisées
Client de services Web (SOAP)	Any	Equilibreur de charge Apache	80	TCP	Apache httpd.conf	Port de l'équilibreur de charge Apache pour les communications de base
Client de services Web (SOAP)	Any	Equilibreur de charge Apache	443	TCP	Apache httpd.conf	Port de l'équilibreur de charge Apache pour les communications sécurisées
Client Catalyst REST	Any	Equilibreur de charge Apache	7000	HTTP	node0-config.xml, http.port	Port du conteneur Catalyst de CA Process Automation
Client Catalyst REST	Any	Equilibreur de charge Apache	7443	HTTPS	node0-config.xml, https.port	Port sécurisé du conteneur Catalyst de CA Process Automation

De	Port	Au	Port d'écoute par défaut	Protocol	Configuration	Description
Navigateur Web (administrateur CA Catalyst)	Any	orchestrateur	8181	TCP	ucf.pax.web.http.port	Interface d'administration de CA Catalyst : non utilisée dans les opérations standard.

Annexe C: Conservation du nom DNS ou de l'adresse IP de l'orchestrateur

Ce chapitre traite des sujets suivants :

Maintenance des adresses IP (page 247)
Résolution des caractères non valides dans le nom DNS de CA Process Automation (page 248)

Maintenance des adresses IP

La maintenance des adresses IP et/ou des noms peut être nécessaire. Exemples :

- Modifiez l'adresse IP et le nom d'un orchestrateur.

  Modifiez la combinaison nom-adresse IP partout dans les fichiers suivants.

  répertoire_installation/server/c2o/.config/OasisConfig.properties

  répertoire_installation/server/c2o/.config/Domain.xml

  Remarque : Pour continuer d'utiliser un nom d'hôte inchangé dans toutes les références dans CA Process Automation, modifiez le DNS avec la nouvelle adresse IP.

- Si vous installez des agents à l'aide d'adresse IP modifiées, reconfigurez l'agent en procédant à la mise à jour du fichier suivant :

  répertoire_installation/PAM Agent/PAMAgent/.config/OasisConfig.properties

  Modifiez la valeur de la propriété suivante :

  oasis.jxta.host

- Utilisez plusieurs adresses IP pour CA Process Automation lorsque vous avez deux contrôleurs d'interface réseau, un interne et un autre externe.

  Pour lier CA Process Automation à l'adresse IP externe, ajoutez la propriété suivante au fichier OasisConfig.properties :

  jboss.bind.address=*xxx.xxx.xxx.xxx*

Résolution des caractères non valides dans le nom DNS de CA Process Automation

Dans la version 3.1, CA Process Automation prend en charge l'installation d'orchestrateurs dont le nom DNS inclut des caractères interdits, tels que des traits de soulignement (_).

Si vous avez installé un orchestrateur avec un nom d'hôte non valide, vous devez effectuer les actions correctives suivantes :

1. Créez un enregistrement DNS qui mappe le nom d'hôte corrigé vers son adresse IP.

   Pour connaître les normes à respecter, reportez-vous à la section Syntaxe des noms d'hôte DNS (page 250).

2. Créez un enregistrement DNS qui mappe le nom incorrect vers le nom corrigé.

   Voir Activation du DNS pour résoudre un nom d'hôte non valide (page 248)

3. Mettez à jour le fichier OasisConfig.properties avec le nom corrigé.

   Voir Conservation du nom d'hôte DNS (page 249)

Activation du DNS pour résoudre un nom d'hôte non valide

Si vous avez créé un orchestrateur avec un nom d'hôte qui inclut un trait de soulignement ou un autre caractère non valide, vous pouvez prendre des mesures permettant au serveur DNS de résoudre l'adresse IP d'un nom d'hôte non valide. Cela requiert la création de deux enregistrements au niveau du serveur DNS. Le premier enregistrement indique que le nom d'origine non valide est un alias d'un autre nom canonique.

Procédez comme suit :

1. Dans le système de noms de domaine, créez un enregistrement canonique avec le nouveau nom d'hôte (valide).
2. Créez un enregistrement CNAME qui mappe le nom canonique vers le nom d'origine non valide.

Nom	Type	Valeur
my_host.mycompany.com.	CNAME	myhost.mycompany.com
myhost.mycompany.com	A	172.24.36.107

Dans cet exemple, mon_hôte.masociété.com est un alias pour le nom canonique (CNAME) myhost.mycompany.com.

Si le solveur DNS trouve un enregistrement CNAME lors de la demande de saisie de l'enregistrement de ressource d'origine, il redémarre la requête à l'aide du nom CNAME et non pas du nom d'origine. Le nom canonique vers lequel un enregistrement CNAME pointe peut se trouver n'importe où dans le DNS.

Conservation du nom d'hôte DNS

Vous pouvez modifier le nom d'hôte d'un orchestrateur, s'il n'est pas conforme à la syntaxe prise en charge par exemple. Si vous avez installé CA Process Automation à l'aide d'un nom d'hôte DNS non valide contenant des caractères restreints tels que des traits de soulignement, créez un alias conforme aux normes DNS. Remplacez ensuite le nom d'hôte non valide manuellement par cet alias dans votre fichier OasisConfig.properties.

Procédez comme suit :

1. Créez un alias. Voir Activation du DNS pour résoudre un nom d'hôte non valide (page 248).
2. Connectez-vous en tant qu'administrateur au serveur sur lequel l'orchestrateur de domaine est installé.
3. Accédez au dossier suivant, où répertoire_installation fait référence au chemin d'accès où l'orchestrateur de domaine est installé :

   répertoire_installation`/server/c2o/.config`
4. Ouvrez le fichier OasisConfig.properties dans un éditeur.
5. Localisez la propriété suivante à l'aide de l'option Rechercher :

   `oasis.local.hostname`
6. Remplacez la valeur de la propriété par oasis.local.hostname=.
7. Enregistrez le fichier et fermez-le.
8. Redémarrez le service de l'orchestrateur.
   a. Arrêtez l'orchestrateur (page 138).
   b. Démarrez l'orchestrateur (page 139).

Syntaxe des noms d'hôte DNS

Plusieurs emplacements vous permettent d'entrer un nom de domaine complet ou une adresse IP. Si les noms d'hôte DNS incluent un trait de soulignement ou ne sont pas conformes à la syntaxe requise, spécifiez une adresse IP.

Noms d'hôte DNS valides :

- Les noms commençant par un caractère alphabétique.
- Les noms se terminant par un caractère alphanumérique.
- Les noms contenant entre 2 et 24 caractères alphanumériques.
- Les noms contenant le caractère spécial moins (-).

  Important : Le signe moins (-) est le seul caractère spécial valide autorisé dans les noms d'hôte DNS.

Annexe D: Dépannage

Cette section décrit les méthodes de dépannage relatives à CA Process Automation.

Ce chapitre traite des sujets suivants :

Echec d'installation de CA Process Automation (page 251)
Problème possible lors de l'exécution de CA Process Automation sur un serveur VMware avec une interface réseau E1000 (page 252)
Bug Oracle n° 9347941 (page 254)
Restrictions dans Internet Explorer (page 255)
Installation de CA Process Automation dans des environnements réseau à double pile (IPv4 et IPv6) (page 256)
Performances lentes avec MySQL (page 256)
Impossible de créer la base de données d'exécution (page 258)
Impossible d'exécuter des opérateurs Exécuter le script ou Exécuter le programme sur RHEL6 (page 259)

Echec d'installation de CA Process Automation

Symptôme :

Si un échec se produit lors de l'installation initiale de CA Process Automation, les tentatives ultérieures sur le même emplacement renvoient également un échec.

Solution :

Pour réinstaller CA Process Automation, nettoyez les entrées de registre, fichiers et dossiers restant à cet emplacement avant de commencer l'installation, ou utilisez un autre emplacement.

Problème possible lors de l'exécution de CA Process Automation sur un serveur VMware avec une interface réseau E1000

Symptôme :

Les causes premières de ce problème tiennent à des défaillances d'E/S de socket sporadiques et rares, qui peuvent maintenir le logiciel appelant en attente de la fin d'une lecture indéfiniment.

Du point de vue des utilisateurs, cela se traduit par la suspension des processus qui se terminent normalement sans problème. Ces processus reprennent et se terminent comme prévu après un redémarrage de l'orchestrateur CA Process Automation. Ce problème peut affecter un sous-ensemble limité de processus ou tous les processus en cours d'exécution. Il n'est pas lié au temps de disponibilité de l'orchestrateur et peut se manifester après un redémarrage ou après plusieurs jours, plusieurs semaines ou plusieurs mois d'usage normal de l'orchestrateur.

Ce problème a uniquement été constaté dans les environnements exécutant des volumes élevés de processus CA Process Automation. Dans la plupart des environnements comprenant un NIC E1000, le problème n'est jamais survenu ou si rarement, qu'il n'a pas été détecté.

Solution :

Ce problème est très difficile à confirmer. S'il survient, le thread CA Process Automation est souvent bloqué sur une lecture de socket et aucune erreur pertinente n'est écrite dans les fichiers journaux. Pour confirmer le problème, vous devez vérifier une série d'images mémoire de thread Java prises au cours d'une occurrence pour confirmer que l'opérateur est bloqué sur une lecture de socket.

Lorsque des erreurs relatives à ce problème sont observées, elles tendent à indiquer des erreurs de connexion génériques qui peuvent avoir d'autres causes légitimes, mais sans rapport. Exemple d'erreurs :

```
2013-07-24 18:55:23,219 WARN  [org.hibernate.jdbc.AbstractBatcher]
[nPool Worker-23] exception clearing maxRows/queryTimeout
com.microsoft.sqlserver.jdbc.SQLServerException: The connection is
closed.
                at
com.microsoft.sqlserver.jdbc.SQLServerException.makeFromDriverErro
r(Unknown Source)
                at
com.microsoft.sqlserver.jdbc.SQLServerConnection.checkClosed(Unkno
wn Source)
                at
com.microsoft.sqlserver.jdbc.SQLServerStatement.checkClosed(Unknow
n Source)
```

```
                at
com.microsoft.sqlserver.jdbc.SQLServerStatement.getMaxRows(Unknown
Source)
                at
org.jboss.resource.adapter.jdbc.CachedPreparedStatement.getMaxRows
(CachedPreparedStatement.java:367)
                at
org.jboss.resource.adapter.jdbc.WrappedStatement.getMaxRows(Wrappe
dStatement.java:378)
                at
org.hibernate.jdbc.AbstractBatcher.closeQueryStatement(AbstractBat
cher.java:272)
                at
org.hibernate.jdbc.AbstractBatcher.closeQueryStatement(AbstractBat
cher.java:209)
```

. . . and so on.

Dans ce cas, l'identification du problème est difficile et d'autres causes d'échec des communications doivent être exclues.

Un échec de processus fréquent ou l'échec d'un ou de plusieurs opérateurs qui se répète indique probablement que d'autres problèmes sans rapport existent dans la conception du processus ou la fonctionnalité de l'orchestrateur.

Sur les sites où la présence du problème a été confirmée, la reconfiguration du serveur VMware à partir d'un pilote de NIC E1000 vers un pilote de NIC VMXnet-3 offre une solution partielle très efficace.

Cette solution n'est pas considérée par CA Technologies comme une solution complète, car le taux d'incident de ce problème est très faible et le délai entre occurrences est assez long, même avec le NIC E1000.

Si vous voulez vérifier la présence du problème avant d'effectuer la modification du pilote, contactez le support de CA pour obtenir de l'aide lors de la configuration de la journalisation et des images mémoire de thread Java.

Bug Oracle n° 9347941

Important : Lors de l'exécution des versions du SGBDR Oracle antérieures à la version 11.1.0.7, CA Process Automation peut parfois rencontrer le problème connu 9347941 relatif au SGBDR Oracle : l'insertion simultanée de données CLOB dont les valeurs de colonne individuelles sont supérieures à 52 kilo-octets peut parfois occasionner le remplacement de ces données par des espaces. Ce problème survient avec les versions 10 g et 11 g du SGBDR Oracle.

Symptôme :

Le processus CA Process Automation se bloque. Pour que le processus se termine, vous devez le réinitialiser au niveau de l'opérateur où il s'est bloqué. Ce problème est rare et survient uniquement avec des taux extrêmement élevés de contention des mises à jour.

Solution :

Aucun problème n'est survenu avec les versions 11.1.0.7 et 11.2.0.2 d'Oracle. Il est donc recommandé aux sites utilisant Oracle comme bases de données CA Process Automation d'exécuter la version 11.1.0.7, 11.2.0.2 ou une version ultérieure.

Restrictions dans Internet Explorer

Internet Explorer limite l'installation de l'agent en cas d'installation dans un autre réseau que celui dans lequel l'orchestrateur de domaine est installé.

Symptôme :

Accédez à l'Orchestrateur de domaine à l'aide de Internet Explorer et installe l'Agent CA Process Automation dans un réseau autre que le réseau où Orchestrateur de domaine est installé. L'installation peut échouer lors du téléchargement des fichiers JAR à installer.

Solution :

Ce problème est sporadique. Il pourrait s'expliquer par le fait que Java ne parvient pas à charger les fichiers JAR lors du routage via le proxy dans Internet Explorer. Pour atténuer le problème, activez l'option Direct Connect (Connexion directe) dans les paramètres réseau Java avant d'installer l'agent.

Procédez comme suit :

1. Ouvrez le Panneau de configuration Java sur le système hôte où vous installez l'agent.
2. Sous l'onglet General (Général), ouvrez Network Settings (Paramètres réseau).

   La page Network Settings (Paramètres réseau) s'affiche.
3. Sélectionnez l'option Direct Connect (Connexion directe) et cliquez sur OK pour enregistrer les modifications.
4. Installez l'agent.

Installation de CA Process Automation dans des environnements réseau à double pile (IPv4 et IPv6)

Si vous installez CA Process Automation dans des environnements réseau à double pile (IPv4 et IPv6), il se peut que CA Process Automation ne parvienne pas à démarrer.

Symptôme :

Si vous installez CA Process Automation dans des environnements réseau à double pile (IPv4 et IPv6), il se peut que vous rencontriez des problèmes lors de l'ouverture ou de l'accès aux composants CA Process Automation suivants sur le réseau :

- Orchestrateurs de domaine
- Orchestrateurs
- Agents

Solution :

Désactivez pile de IPv6 sur le système hôte sur lequel un des composants CA Process Automation suivants s'exécutent, puis redémarrez les services :

- Orchestrateurs de domaine
- Orchestrateurs
- Agents

Performances lentes avec MySQL

Symptôme :

Lorsque j'installe CA Process Automation avec MySQL ou Oracle en tant que base de données, je remarque un manque de performance.

Solution :

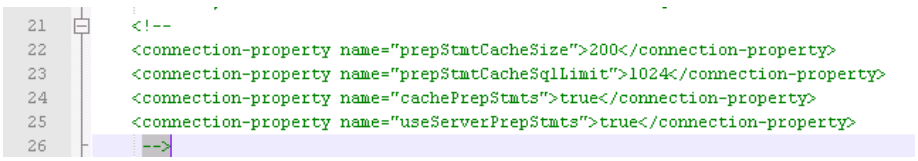
Après l'installation, modifiez le fichier oasis-ds.xml pour améliorer les performances de CA Process Automation.

Procédez comme suit :

1. Localisez et ouvrez le fichier oasis-ds.xml, situé dans :

   répertoire_installation/server/c2o/ext-deploy

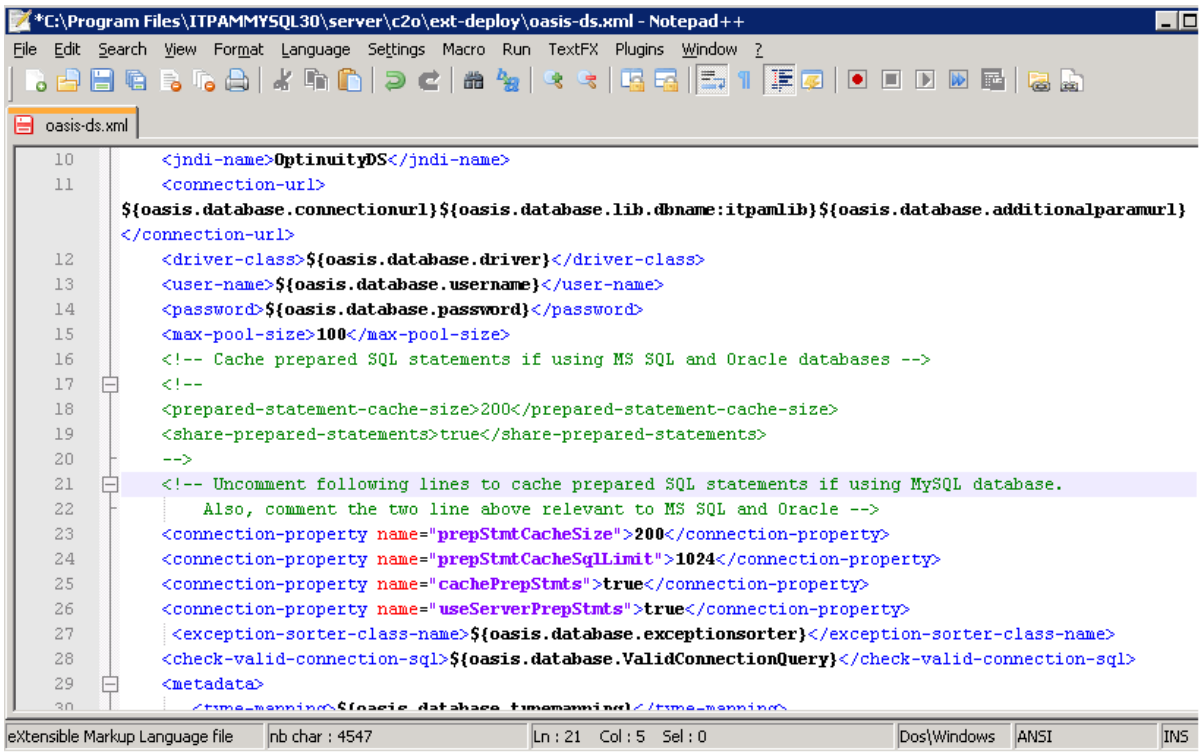
2. Supprimer les lignes de commentaire suivantes :



3. Commentez les lignes suivantes :

```
16      <!-- Cache prepared SQL statements if using MS SQL and Oracle databases -->
17      <prepared-statement-cache-size>200</prepared-statement-cache-size>
18      <share-prepared-statements>true</share-prepared-statements>
```

Le fichier mis à jour devrait ressembler à ceci :



4. Redémarrez l'orchestrateur.

Impossible de créer la base de données d'exécution

Symptôme :

Lorsque j'installe un orchestrateur et que j'indique la base de données d'exécution dans la fenêtre Base de données d'exécution, l'exception suivante est levée :

```
La base de données d'exécution est utilisée par un autre orchestrateur.
```

Solution :

La version 4.0 de CA Process Automation ne permet pas de partager la même base de données d'exécution entre différents orchestrateurs. La solution habituelle consiste à créer la base de données d'exécution sous un autre nom ou à l'héberger sur un autre serveur de base de données.

Procédez comme suit **uniquement** si vous voulez conserver les informations d'exécution de la base de données dans une nouvelle instance CA Process Automation. C'est rarement le cas et la réinitialisation de RuntimeDbOrchestratorID comporte plusieurs effets secondaires indésirables, notamment le fait de rendre l'exécution des opérateurs impossible dans la base de données d'exécution à terminer. Entre autres inconvénients, tous les agents et les orchestrateurs secondaires doivent également être réinstallés. Si vous doutez de la validité de cette procédure pour résoudre votre problème, consultez le support technique avant de poursuivre.

Dans cette version, une nouvelle table Propriétés est créée dans la base de données avec les colonnes suivantes :

- PropKey
- PropValue

Chaque fois qu'un orchestrateur utilise une base de données d'exécution, une nouvelle ligne est insérée dans la table Propriétés. La PropKey est RuntimeDbOrchestratorID et la PropValue est l'ID unique de l'orchestrateur.

Lorsqu'un autre orchestrateur sollicite la même base de données, celle-ci est validée dans la table Propriétés. Si l'ID unique de l'orchestrateur qui effectue la demande ne correspond pas à Propvalue, le message suivant s'affichera :

```
La base de données d'exécution est utilisée par un autre orchestrateur.
```

Important : Les entrées de base de données d'exécution ne sont pas supprimées, même après la désinstallation du produit.

Pour utiliser à nouveau la même base de données pour l'exécution, exécutez la requête SQL suivante et supprimez la ligne correspondante de la table Propriétés.

```
delete from properties where propkey = 'RuntimeDbOrchestratorID'
```

Impossible d'exécuter des opérateurs Exécuter le script ou Exécuter le programme sur RHEL6

Symptôme :

Un échec se produit lors de l'exécution des opérateurs Exécuter le script ou Exécuter le programme sur RHEL6.

Solution :

Ces opérateurs recherchent le shell Korn (ksh) lorsqu'ils sont exécutés sur des plates-formes UNIX ou Linux. Par défaut, ksh n'est pas installé sur RHEL 6.

Vous pouvez résoudre ce problème en effectuant l'une des opérations suivantes :

- Installation de ksh :

  vous pouvez installer ksh à l'aide de la commande suivante :

  ```
  yum install ksh
  ```

- Pointage d'un lien symbolique vers un shell valide

  Créez un lien symbolique /bin/ksh et mappez-le de la même façon vers un shell, tel que Bash, qui existe sur l'ordinateur. Utilisez cette commande, où /bin/bash correspond à l'emplacement du shell Bash :

  ```
  ln -s /bin/bash /bin/ksh
  ```

Annexe E: Equilibreur de charge Apache

L'équilibreur de charge Apache ne prend *pas* en charge la méthode de communication simplifiée pour les agents. Pour utiliser la communication simplifiée, vous devez utiliser NGINX ou un autre équilibreur de charge basé sur un socket Web. Si vous utilisez la méthode de communication désapprouvée, utilisez ces instructions pour installer et configurer l'équilibreur de charge Apache.

Pour plus d'informations, consultez la rubrique A propos des communications d'agent (page 159).

Conditions requises pour l'équilibreur de charge Apache

Un *orchestrateur mis en cluster* est un ensemble de noeuds qui s'affiche et agit comme un orchestrateur unique, et qui utilise une bibliothèque partagée. Vous pouvez mettre en cluster un orchestrateur CA Process Automation pour garantir une haute disponibilité, la tolérance aux pannes et la modularité.

Un équilibreur de charge, tel que le serveur HTTP Apache, est requis pour mettre en cluster un orchestrateur, y compris l'orchestrateur de domaine. Aucun équilibreur de charge ne fait partie de l'installation CA Process Automation.

Même si l'équilibreur de charge peut être configuré sur le même hôte que celui hébergeant les noeuds d'orchestrateur, il est plutôt recommandé de l'installer sur un hôte distinct.

Un équilibreur de charge est *uniquement* requis pour un orchestrateur dans une configuration en cluster et dans certaines configurations d'authentification unique.

Important : Si un orchestrateur est installé et configuré avant un équilibreur de charge, vous ne pouvez pas le mettre en cluster ultérieurement.

Configuration de l'équilibreur de charge Apache sur Windows

Cette section fournit des instructions relatives à l'installation et à la configuration de l'équilibreur de charge Apache sur Windows.

Vous pouvez réaliser la configuration dans l'un des modes suivants :

- Configuration de base (Windows) (page 262)
- Configuration sécurisée (Windows) (page 266)

Configuration de base (Windows)

Cette section fournit des instructions relatives à l'installation et à la configuration de l'équilibreur de charge Apache en mode de base.

Remarque : Vous pouvez utiliser un équilibreur de charge autre que l'équilibreur de charge Apache. Toutefois, un orchestrateur CA Process Automation requiert que certaines classes de demande soient dirigées vers un noeud spécifique de l'orchestrateur mis en cluster. Par conséquent, l'équilibrage de charge simple est insuffisant. Pour d'autres solutions, consultez la page CA Process Automation Best Practices (Meilleures pratiques relatives à CA Process Automation) ou contactez le support CA. La bibliothèque inclut des liens vers ces pages.

Procédez comme suit :

1. Installation d'un équilibreur de charge et préparation des modèles de configuration (Windows) (page 262).
2. Configurez les communications de base (page 264).
3. (Facultatif) Configurez l'équilibreur de charge Apache pour l'API Catalyst RESTful (Windows) (page 265)

   Remarque : Pour qu'un serveur Web Apache puisse transférer des demandes HTTPS à des opérateurs Catalyst, les certificats SSL doivent être au format PEM. Si nécessaire, générez des fichiers de certificat SS (page 50)L.

Installation d'un équilibreur de charge et préparation des modèles de configuration (Windows)

Le support d'installation CA Process Automation inclut l'exemple de fichier de configuration suivant pour l'équilibreur de charge Apache que vous pouvez utiliser comme référence pour la configuration.

```
ApacheConfig.zip
```

Les instructions suivantes supposent qu'un équilibreur de charge Apache 2.2 est dédié à CA Process Automation. En premier lieu, installez un équilibreur de charge Apache. Puis, extrayez les fichiers à partir du fichier ZIP ApacheConfTemplates de CA Process Automation dans le dossier Conf, sous le dossier d'installation Apache.

Procédez comme suit :

1. Connectez-vous à l'hôte sur lequel l'équilibreur de charge s'exécute.

   Généralement, l'équilibreur de charge se trouve sur le même hôte que votre orchestrateur de domaine. Toutefois, l'hôte hébergeant l'orchestrateur de domaine doit pouvoir être routé à partir de l'équilibreur de charge.
2. Téléchargez et installez le dernier équilibreur de charge Apache offrant une prise en charge SSL. Suivez les instructions du fournisseur.

3. Téléchargez le fichier suivant pour la version d'Apache que vous avez installée :

   `mod_jk.so`

   Télécharger la dernière version est recommandé.

4. Copiez le fichier mod_jk.so dans le dossier suivant :

   répertoire_installation_apache`\modules`

5. Accédez au dossier suivant dans le média d'installation CA Process Automation :

   répertoire_installation`\DVD1\ApacheConfTemplates`

6. Extrayez les fichiers suivants d'ApacheConfig.zip :

   `mod-jk.conf`

   `httpd-proxy.conf`

   `uriworkermap.properties`

   `workers.properties`

   `httpd VIRTUALHOST_EXAMPLE`

   Remarque : Le fichier VIRTUALHOST_EXAMPLE FILE HTTPD extrait contient du texte que vous pouvez couper et coller dans le fichier HTTPD d'Apache lorsque vous configurez des communications sécurisées. Le texte requis est également inclus dans la documentation.

7. Copiez les fichiers extraits suivants dans le dossier *répertoire_installation_apache*\conf :

   `mod-jk.conf`

   `httpd-proxy.conf`

   `uriworkermap.properties`

   `workers.properties`

   Remarque : Si vous ne disposez d'aucun équilibreur de charge Apache 2.2 dédié, fusionner les informations de configuration de l'exemple de propriétés de modèle et les fichiers Conf dans vos fichiers existants. Par mesure de précaution, sauvegardez vos fichiers avant de les modifier.

Configuration des communications de base

Vous pouvez configurer un équilibreur de charge pour les communications de base avec les noeuds de l'orchestrateur de domaine ou avec d'autres orchestrateurs.

Procédez comme suit :

1. Accédez au dossier suivant :

   répertoire_installation_apache\conf

   Ce dossier contient les fichiers worker.properties et mod-jk.conf.
2. Ouvrez le fichier workers.properties.
3. Ajoutez le premier noeud en définissant node1 qui commence par la ligne suivante :
   worker.**node1**.host=<Entrez le nom d'hôte du noeud 1 ici>
4. A partir de cette ligne, remplacez l'espace réservé *Entrez le nom d'hôte du noeud 1 ici* pour worker.node1.host par la valeur valide.

   Remarque : Les valeurs valides sont l'adresse IP, le nom de domaine complet ou l'alias de DNS qui pointe vers l'hôte sur lequel vous installez le noeud Orchestrateur de domaine initial. La valeur valide est la même que celle utilisée pour Hôte de serveur lors de l'installation de l'orchestrateur de domaine.
5. Enregistrez et fermez le fichier worker.properties.
6. Ouvrez le fichier mod-jk.conf.
7. Supprimez la ligne de commentaire suivante :

   # JkMountFile conf/uriworkermap.properties
8. Enregistrez et fermez le fichier mod-jk.conf.
9. Ouvrez le fichier httpd.conf.
10. Ajoutez l'entrée suivante à la fin du fichier httpd.conf :
    Module d'équilibrage #Load
    Inclure conf/mod-jk.conf
11. Enregistrez et fermez le fichier httpd.conf.

Configuration de l'équilibreur de charge Apache pour l'API Catalyst RESTful (Windows)

Vous pouvez configurer le serveur Web Apache (équilibreur de charge) pour l'API Catalyst RESTful. La configuration d'Apache est modifiée en fonction de l'équilibreur de charge Apache qui est déjà configuré pour CA Process Automation.

Lorsque vous avez configuré CA Process Automation en mode de cluster, effectuez les tâches postérieures à l'installation.

Procédez comme suit :

1. Accédez au dossier suivant sur le support d'installation de CA Process Automation :

   répertoire_installation\DVD1\ApacheConfTemplates

2. Extrayez les fichiers suivants d'ApacheConfig.zip :

   `httpd-proxy.conf`

3. Copiez le fichier httpd-proxy.conf dans le répertoire *apacheHome*/conf/extra.

4. Mettez à jour les lignes suivantes sur les hôtes virtuels HTTP et HTTPS, afin de remplacer les noms d'hôte d'orchestrateur pour BalancerMember.

   Membres de noeud non sécurisé

   ```
   <Proxy balancer://ucfcluster>
   BalancerMember  http://< Enter node1 hostname>:7000
   BalancerMember  http://< Enter node2 hostname>:7000
   ```

   Membres de noeud sécurisé

   ```
   <Proxy balancer://sslcluster>
   BalancerMember  https://< Enter node1 hostname>:7443
   BalancerMember  https://< Enter node2 hostname>:7443
   ```

5. Remplacez l'espace réservé <Enter node*x* hostname> de worker.node*x*.host par la valeur valide.

   Remarque : Les valeurs valides sont l'adresse IP, le nom de domaine complet ou l'alias de DNS qui pointe vers l'hôte sur lequel vous installez le noeud Orchestrateur de domaine initial. La valeur valide est la même que celle utilisée pour Hôte de serveur lors de l'installation de l'orchestrateur de domaine.

6. Enregistrez le fichier httpd-proxy.conf.

7. Ouvrez le fichier *apacheHome*/conf/httpd.conf et vérifiez que les ports 7000 et 7443 ne sont pas utilisés.

8. Ajoutez la ligne suivante à la fin du fichier httpd.conf :

   `Incluez conf/extra/httpd-ssl.conf.`

9. Suivez la procédure de la section Génération de fichiers de certificat SSL (page 50) pour générer les fichiers c2okey2.pem et c2ocert.pem.

10. Copiez les fichiers générés dans le répertoire *apacheHome/*conf.

11. Enregistrez les fichiers modifiés, puis redémarrez le serveur Web Apache.

Configuration sécurisée (Windows)

Cette section fournit des instructions relatives à l'installation et à la configuration de l'équilibreur de charge Apache en mode sécurisé.

Procédez comme suit :

1. Installez un équilibreur de charge et préparez les modèles de configuration (page 262).
2. Génération de fichiers de certificat SSL (page 50)

   Remarque : Pour qu'un serveur Web Apache puisse transférer des demandes HTTPS à des opérateurs Catalyst, les certificats SSL doivent être au format PEM.
3. Configuration des communications sécurisées (Windows) (page 268).
4. Configuration de l'équilibreur de charge Apache pour l'API Catalyst RESTful (Windows) (page 265)

Génération de fichiers de certificat SSL

Les certificats SSL doivent être générés *après* l'installation de CA Process Automation, mais *avant* la configuration de la communication sécurisée pour votre équilibreur de charge. Les certificats SSL ne sont pas requis si vous voulez utiliser la communication simple, non sécurisée pour votre équilibreur de charge.

Une fois générés, l'emplacement des fichiers de certificat doit être identifié lors de la configuration de l'équilibreur de charge pour la communication sécurisée.

Procédez comme suit :

1. Téléchargez et installez OpenSSL à partir d'un fournisseur tiers.

   Remarque : Assurez-vous que le kit de développement Java (JDK) est installé sur l'hôte sur lequel vous installez OpenSSL.

2. A l'issue de l'installation de CA Process Automation en mode de cluster (avec au moins un noeud), l'assistant d'installation de CA Process Automation génère le fichier c2okeystore à l'emplacement suivant :

   ```
   \server_location\c2o\.config
   ```

   Copiez le fichier c2okeystore et collez-le dans le répertoire suivant :

   ```
   \jdk_location\bin
   ```

   Vous pouvez exécuter les commandes localement à partir de cet emplacement.

3. Utilisez l'utilitaire Keytool du JDK pour importer le magasin de clés au format pksc12, en procédant comme suit :

   a. Accédez au répertoire jdk_location\bin et exécutez la commande suivante :

      ```
      keytool -importkeystore -srckeystore c2okeystore
      -srcstoretype jks -destkeystore c2okeystore.p12
      -deststoretype pkcs12
      ```

      La console vous invite à saisir le mot de passe du magasin de clés de destination.

      Remarque : Le fichier OasisConfig.properties contient le mot de passe du magasin de clés. Recherchez le fichier dans ce répertoire : `\server_location\c2o\.config\`

      Ouvrez le fichier et copiez le mot de passe. La valeur se trouve à côté de l'entrée KEYSTOREID=.

      Par exemple : KEYSTOREID=723e1830-a98c-49a1-8f16-a0794c872835. Le mot de passe est 723e1830-a98c-49a1-8f16-a0794c872835.

   b. Collez le mot de passe dans l'invite de mot de passe du magasin de clés de destination dans votre console ouverte.

   c. Lorsque vous y êtes invité, ressaisissez le mot de passe.

   d. A l'invite de mot de passe de la clé de source, entrez le mot de passe à nouveau.

      Un fichier c2okeystore.p12 est généré dans le répertoire \jdk_location\bin.

   e. Vous devez convertir le magasin de clés au format p12 en fichiers de clé et de certificat au format PEM. Pour cela, exécutez la commande openssl à l'emplacement du répertoire \jdk_location\bin :

      ```
      openssl pkcs12 -nocerts -in c2okeystore.p12 -out c2okey.pem
      ```

   f. Lorsque l'invite Import Password (Importer un mot de passe) s'ouvre, entrez le mot de passe du magasin de clés.

g. Lorsque l'invite Phrase secrète s'ouvre, entrez une expression.

h. Ressaisissez la phrase secrète PEM.

i. A l'emplacement du répertoire \jdk_location\bin, exécutez la commande suivante :
```
openssl pkcs12 -clcerts -in c2okeystore.p12 -out c2ocert.pem
```

j. Lorsque l'invite Import Password (Importer un mot de passe) s'ouvre, entrez le mot de passe du magasin de clés.

k. Lorsque l'invite Phrase secrète s'ouvre, saisissez l'expression créée à l'étape g.

l. Ressaisissez la phrase secrète PEM.

m. A l'emplacement du répertoire \jdk_location\bin, exécutez la commande suivante :
```
openssl rsa -in c2okey.pem -out c2okey2.pem
```

n. Lorsque l'invite Phrase secrète s'ouvre, saisissez l'expression créée à l'étape g.

o. Ressaisissez la phrase secrète PEM.

p. Copiez les fichiers c2okey2.pem et c2ocert.pem dans le répertoire \conf de votre équilibreur de charge.

Remarque : Effectuez une sauvegarde de ces fichiers.

Configuration des communications sécurisées (Windows)

Vous pouvez configurer un équilibreur de charge pour qu'il utilise une communication sécurisée. Dans les étapes suivantes, *certloc* fait référence à votre emplacement de certificat.

Procédez comme suit :

1. Installez un équilibreur de charge et préparez les modèles de configuration (page 262).
2. Ouvrez le fichier workers.properties.
3. Ajoutez le premier noeud en définissant node1 qui commence par la ligne suivante :
```
worker.node1.host=<Entrez le nom d'hôte du noeud 1 ici>
```
4. A partir de cette ligne, remplacez l'espace réservé *Entrez le nom d'hôte du noeud 1 ici* de worker.node1.host par la valeur valide.

   Remarque : Les valeurs valides sont l'adresse IP, le nom de domaine complet ou l'alias de DNS qui pointe vers l'hôte sur lequel vous installez le noeud Orchestrateur de domaine initial. La valeur valide est la même que celle utilisée pour Hôte de serveur lors de l'installation de l'orchestrateur de domaine.
5. Enregistrez et fermez le fichier de travail.

6. Passez en revue les emplacements par défaut CA dans le fichier openssl dans le répertoire suivant.

   répertoire_installation_apache/conf

7. Créez ou obtenez un fichier de certificat et un fichier de clé privée avec un nom commun (Common Name) correspondant au nom de serveur (ServerName) dans httpd.conf.

   Par exemple, les étapes suivantes décrivent l'utilisation de l'utilitaire openssl fourni par l'équilibreur de charge Apache pour créer un fichier de certificat. Des options supplémentaires permettent de contrôler l'expiration du certificat, les noms de fichier et les algorithmes. Si votre site requiert une configuration spéciale, reportez-vous à la documentation proposée par le fournisseur.

   a. Ouvrez une invite de commande

   b. Remplacez les répertoires par le dossier bin Apache.

      cd *répertoire_installation_apache*/bin

   c. Créez un fichier CSR (demande de signature de certificat) et des fichiers PEM. Pour ce faire, saisissez la commande suivante en remplaçant mypamserver par le nom de votre choix.

      openssl req -config ../conf/openssl.cnf -new -out *mypamserver*.csr

      Vous êtes invité à saisir la phrase secrète associée au fichier PEM, ainsi que d'autres informations d'identification.

      - Vous pouvez accepter les valeurs par défaut pour la plupart des informations d'identification (par exemple, nom de pays, nom d'état ou de région, nom de région, nom d'organisation et nom d'unité organisationnelle). Pour laisser un champ vide, entrez un point (.).
      - Lorsque l'invite Common Name (Nom commun) s'affiche, entrez la portion de nom d'hôte de ServerName comme valeur dans *répertoire_installation_apache/*conf/httpd.conf.

        Par exemple, si la valeur ServerName dans httpd.conf est myhost.mycompany.com:80, spécifiez **myhost.mycompany.com** comme Nom commun (Common Name).
      - Les champs suivants sont facultatifs : Adresse électronique, Dir (Répertoire), Challenge password (Mot de passe de vérification) et Company Name (Nom de société).

      L'équilibreur de charge Apache crée les fichiers *mypamserver.*csr et *privkey.*pem dans le répertoire actuel.

d. Créez votre clé RSA privée. Pour ce faire, entrez la phrase secrète associée à *privkey*.pem lorsque l'équilibreur de charge vous la demande.

```
openssl rsa -in privkey.pem -out mypamserver.key
```

e. Créez votre certificat.

```
openssl x509 -in mypamserver.csr -out mypamserver.cert -req
-signkey mypamserver.key
```

8. Clôturez l'invite de commande et ouvrez l'explorateur Windows pour copier et supprimer les fichiers générés :

   a. Sélectionnez le dossier *certloc* ou créez un dossier pour y placer le certificat et les fichiers de clé privée.

   b. Ouvrez le dossier *répertoire_installation_apache*\bin, où les fichiers CERT et KEY ont été générés.

   c. Glissez-déposez les fichiers *mypamserver*.cert et *mypamserver*.key dans le dossier *certloc*.

   d. Supprimez les fichiers intermédiaires créés dans le dossier *répertoire_installation_apache/*bin. Il s'agit des fichiers *mypamserver*.CSR, *privkey*.PEM et .RND.

9. Sauvegardez les fichiers que vous avez créés.

10. A l'aide d'un éditeur de texte, modifiez le fichier de texte HTTPD (*répertoire_installation_apache*\conf\httpd.conf) comme suit :

    a. Supprimer les lignes de commentaire suivantes :

    ```
    Loadmodule rewrite_module modules/mod_rewrite.so
    ```

    ```
    LoadModule ssl_module modules/mod_ssl.so
    ```

    ```
    Incluez conf/extra/httpd-ssl.conf
    ```

    b. Ajoutez les lignes suivantes à la fin du fichier httpd.conf. Vous pouvez copier et coller le texte à partir du fichier HTTPD VIRTUALHOST_EXAMPLE que vous avez extrait du dossier compressé SecureDomainConfig_Template.zip.

    ```
    <VirtualHost *:80>
    JkMountFile conf/uriworkermap.properties
    RewriteEngine On
    RewriteCond %{HTTPS} off
    RewriteCond http://%{HTTP_HOST}%{REQUEST_URI}
    !^http://.*c2orepository*|MirroringRequestProcessor*|mirror
    ingrepository*|StartAgent*|genericNoSecurity*|soapAttachmen
    t*
    RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
    </VirtualHost>
    Module d'équilibrage #Load
    Inclure conf/mod-jk.conf
    ```

    c. Enregistrez le fichier httpd.conf modifié et fermez l'éditeur.

11. Sauvegardez les fichiers que vous avez modifiés.
12. A l'aide d'un éditeur de texte, apportez les modifications suivantes au fichier de configuration *répertoire_installation_apache/*conf/extra/httpd-ssl.conf :
    a. Supprimez les marques de commentaire (le cas échéant) dans le texte suivant : Listen 443
    b. Remplacez l'emplacement SSLCertificateFile par .../*certloc/mypamserver.*cert.

       ```
       SSLCertificateFile "C:/certloc/mypamserver.cert"
       ```

    c. Remplacez l'emplacement SSLCertificateKeyFile par .../*certloc/mypamserver.*key.

       ```
       SSLCertificateKeyFile "C:/certloc/mypamserver.key"
       ```

    d. Ajoutez les lignes suivantes à la fin de l'élément <VirtualHost>, avant l'élément </VirtualHost> :

       ```
       SSLOptions +StdEnvVars +ExportCertData
       JkMountFile conf/uriworkermap.properties
       ```

    e. Enregistrez le fichier httpd.conf-ssl modifié et fermez l'éditeur.
13. Redémarrez le service Apache. Pour ce faire, dans le menu Démarrer, cliquez sur Programmes, Apache HTTP Server 2.2, Control Apache Server (Contrôler le serveur Apache), Redémarrer.

    Les modifications sont appliquées.

Configuration de l'équilibreur de charge Apache sur un système d'exploitation autre que Windows

Cette section fournit des instructions relatives à l'installation et à la configuration de l'équilibreur de charge Apache sur un système d'exploitation autre que Windows.

Vous pouvez réaliser la configuration dans l'un des modes suivants :

- Configuration de base (système d'exploitation autre que Windows) (page 272)
- Configuration sécurisée (système d'exploitation autre que Windows) (page 276)

Configuration de base (système d'exploitation autre que Windows)

Cette section fournit des instructions relatives à l'installation et à la configuration de l'équilibreur de charge Apache en mode de base.

Remarque : Vous pouvez utiliser un équilibreur de charge autre que l'équilibreur de charge Apache. Toutefois, un orchestrateur CA Process Automation requiert que certaines classes de demande soient dirigées vers un noeud spécifique de l'orchestrateur mis en cluster. Par conséquent, l'équilibrage de charge simple est insuffisant. Pour d'autres solutions, consultez la page CA Process Automation Best Practices (Meilleures pratiques relatives à CA Process Automation) ou contactez le support CA. La bibliothèque inclut des liens vers ces pages.

Procédez comme suit :

1. Installation d'un équilibreur de charge et préparation des modèles de configuration (système d'exploitation autre que Windows) (page 272).
2. Configurez les communications de base (page 264).
3. Configuration de l'équilibreur de charge Apache pour l'API Catalyst RESTful (système d'exploitation autre que Windows) (page 274)

   Remarque : Pour qu'un serveur Web Apache puisse transférer des demandes HTTPS à des opérateurs Catalyst, les certificats SSL doivent être au format PEM. Si nécessaire, générez des fichiers de certificat SS (page 50)L.

Installation d'un équilibreur de charge et préparation des modèles de configuration (système d'exploitation autre que Windows).

Le support d'installation CA Process Automation inclut l'exemple de fichier de configuration suivant pour l'équilibreur de charge Apache que vous pouvez utiliser comme référence pour la configuration.

`ApacheConfig.zip`

Les instructions suivantes supposent qu'un équilibreur de charge Apache 2.2 est dédié à CA Process Automation. En premier lieu, installez un équilibreur de charge Apache. Puis, extrayez les fichiers à partir du fichier ZIP ApacheConfTemplates de CA Process Automation dans le dossier Conf, sous le dossier d'installation Apache.

Procédez comme suit :

1. Connectez-vous à l'hôte sur lequel l'équilibreur de charge s'exécute.

   Généralement, l'équilibreur de charge se trouve sur le même hôte que votre orchestrateur de domaine. Toutefois, l'hôte hébergeant l'orchestrateur de domaine doit pouvoir être routé à partir de l'équilibreur de charge.

2. Téléchargez et installez l'équilibreur de charge Apache le plus récent. Par exemple, accédez au dossier extrait et exécutez les commandes suivantes :

   ```
   ./configure -prefix=<install location>-enable-so -enable-mods-shared=all
   -enable-mod-rewrite --with-z=<zlib home>--with-included-apr  --with-mpm=worker
   --enable-ssl --with-ssl=<ssl home>
   ```

   ```
   Make
   ```

   ```
   Make install
   ```

3. Téléchargez et installez le connecteur Tomcat vers le module mod_jk. Par exemple, accédez au répertoire *<emplacement d'extraction du connecteur Tomcat>/*native/ et exécutez les commandes suivantes :

   ```
   ./configure --with-apxs=<install location>/bin/apxs
   Make
   Make install
   ```

4. Vérifiez le bon fonctionnement du serveur Apache.

5. Accédez au dossier suivant sur le support d'installation de CA Process Automation :

   répertoire_installation\DVD1\ApacheConfTemplates

6. Extrayez les fichiers suivants d'ApacheConfig.zip :

   ```
   mod-jk.conf
   ```

   ```
   httpd-proxy.conf
   uriworkermap.properties
   workers.properties
   httpd VIRTUALHOST_EXAMPLE
   ```

   Remarque : Le fichier HTTPD extrait contient le texte que vous pouvez couper et coller dans le fichier HTTPD d'Apache lorsque vous configurez des communications sécurisées. Le texte requis est également inclus dans la documentation.

7. Copiez les fichiers extraits dans le dossier suivant :

   répertoire_installation_apache\conf

Configuration de l'équilibreur de charge Apache pour l'API Catalyst RESTful (système d'exploitation autre que Windows)

Vous pouvez configurer le serveur Web Apache (équilibreur de charge) pour l'API Catalyst RESTful. Modifiez la configuration d'Apache en fonction de l'équilibreur de charge Apache qui est déjà configuré pour CA Process Automation.

Assurez-vous que les fichiers binaires suivants sont installés sur le serveur Apache.

```
mod_proxy.so
mod_proxy_balancer.so
mod_proxy_http.so
```

Procédez comme suit :

1. Accédez au dossier suivant sur le support d'installation de CA Process Automation :

   répertoire_installation\DVD1\ApacheConfTemplates

2. Extrayez le fichier suivant d'ApacheConfig.zip :

   `httpd-proxy.conf`

3. Copiez httpd-proxy.conf dans le répertoire suivant :

   `apacheHome/conf/extra`

4. Ouvrez httpd-proxy.conf et commentez les lignes suivantes :

   ```
   LoadModule proxy_module modules/mod_proxy.so
   LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
   LoadModule proxy_http_module modules/mod_proxy_http.so
   ```

5. Revenez au dossier *répertoire_installation_apache*\conf, ouvrez httpd.conf et supprimez les marques de commentaire des lignes suivantes (le cas échéant) :

   ```
   LoadModule proxy_module modules/mod_proxy.so
   LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
   LoadModule proxy_http_module modules/mod_proxy_http.so
   ```

6. Mettez à jour les lignes suivantes sur les hôtes virtuels HTTP et HTTPS, afin de remplacer les noms d'hôte d'orchestrateur pour BalancerMember.

   Membres de noeud non sécurisé

   - Noeud 1

     `BalancerMember  http://< Enter node1 hostname>:7000`

   - Noeud 2

     `BalancerMember  http://< Enter node2 hostname>:7000`

Membres de noeud sécurisé

- Noeud 1

  ```
  BalancerMember  https://< Enter node1 hostname>:7443
  ```

- Noeud 2

  ```
  BalancerMember  https://< Enter node2 hostname>:7443
  ```

7. Remplacez l'espace réservé Entrez le nom d'hôte du noeud 1 ici par la valeur valide.

   Remarque : Les valeurs valides sont l'adresse IP, le nom de domaine complet ou l'alias de DNS qui pointe vers l'hôte sur lequel vous installez le noeud Orchestrateur de domaine initial. La valeur valide est la même que celle utilisée pour Hôte de serveur lors de l'installation de l'orchestrateur de domaine.

8. Enregistrez le fichier httpd-proxy.conf.
9. Ouvrez le fichier apacheHome/conf/httpd.conf et vérifiez que les ports 7000 et 7443 ne sont pas utilisés.
10. Ajoutez la ligne suivante à la fin du fichier httpd.conf :

    ```
    Incluez conf/extra/httpd-ssl.conf.
    ```

11. Générez des fichiers de certificat SSL (page 50) pour générer les fichiers c2okey2.pem et fichiers c2ocert.pem.
12. Copiez les fichiers générés dans le répertoire *apacheHome/*conf.
13. Redémarrez le serveur Web Apache.

Configuration sécurisée (système d'exploitation autre que Windows)

Cette section fournit des instructions relatives à l'installation et à la configuration de l'équilibreur de charge Apache en mode sécurisé.

Remarque : Vous pouvez utiliser un équilibreur de charge autre que l'équilibreur de charge Apache. Toutefois, un orchestrateur CA Process Automation requiert que certaines classes de demande soient dirigées vers un noeud spécifique de l'orchestrateur mis en cluster. Par conséquent, l'équilibrage de charge simple est insuffisant. Pour d'autres solutions, consultez la page CA Process Automation Best Practices (Meilleures pratiques relatives à CA Process Automation) ou contactez le support CA. La bibliothèque inclut des liens vers ces pages.

Procédez comme suit :

1. Installation d'un équilibreur de charge et préparation des modèles de configuration (système d'exploitation autre que Windows) (page 272).
2. Configuration des communications sécurisées (système d'exploitation autre que Windows) (page 277).
3. Configuration de l'équilibreur de charge Apache pour l'API Catalyst RESTful (système d'exploitation autre que Windows) (page 274)

   Remarque : Pour qu'un serveur Web Apache puisse transférer des demandes HTTPS à des opérateurs Catalyst, les certificats SSL doivent être au format PEM. Si nécessaire, régénérez des fichiers de certificat SSL (page 50).

Configuration des communications sécurisées (système d'exploitation autre que Windows)

Vous pouvez configurer un équilibreur de charge pour qu'il utilise une communication sécurisée. Dans les étapes suivantes, *certloc* fait référence à votre emplacement de certificat.

Procédez comme suit :

1. Installez un équilibreur de charge et préparez les modèles de configuration (page 262).
2. Ouvrez le fichier workers.properties.
3. Ajoutez le premier noeud en définissant node1 qui commence par la ligne suivante :

   ```
   worker.node1.host=<Entrez le nom d'hôte du noeud 1 ici>
   ```

4. A partir de cette ligne, remplacez l'espace réservé *Entrez le nom d'hôte du noeud 1 ici* pour worker.node1.host par la valeur valide.

   Remarque : Les valeurs valides sont l'adresse IP, le nom de domaine complet ou l'alias de DNS qui pointe vers l'hôte sur lequel vous installez le noeud Orchestrateur de domaine initial. La valeur valide est la même que celle utilisée pour Hôte de serveur lors de l'installation de l'orchestrateur de domaine.

5. Enregistrez et fermez le fichier de travail.
6. Passez en revue les emplacements par défaut CA dans le fichier openssl dans le répertoire suivant.

   répertoire_installation_apache/conf

7. Créez ou obtenez un fichier de certificat et un fichier de clé privée avec un nom commun (Common Name) correspondant au nom de serveur (ServerName) dans httpd.conf.

   Par exemple, les étapes suivantes décrivent l'utilisation de l'utilitaire openssl fourni par l'équilibreur de charge Apache pour créer un fichier de certificat. Des options supplémentaires permettent de contrôler l'expiration du certificat, les noms de fichier et les algorithmes. Si votre site requiert une configuration spéciale, reportez-vous à la documentation proposée par le fournisseur.

   a. Ouvrez une invite de commande

   b. Remplacez les répertoires par le dossier bin Apache.

      cd *répertoire_installation_apache*/bin

c. Créez un fichier CSR (demande de signature de certificat) et des fichiers PEM. Pour ce faire, saisissez la commande suivante en remplaçant mypamserver par le nom de votre choix.

```
openssl req -new -out mypamserver.csr
```

Vous êtes invité à saisir la phrase secrète associée au fichier PEM, ainsi que d'autres informations d'identification.

- Vous pouvez accepter des valeurs par défaut pour la plupart des informations d'identification (par exemple, nom de pays, nom d'état ou de région, nom de région, nom d'organisation et nom d'unité organisationnelle). Pour laisser un champ vide, entrez un point (.).
- Lorsque l'invite Common Name (Nom commun) s'affiche, entrez la portion de nom d'hôte de ServerName comme valeur dans *répertoire_installation_apache/*conf/httpd.conf.

  Par exemple, si la valeur ServerName dans httpd.conf est myhost.mycompany.com:80, spécifiez **myhost.mycompany.com** comme Nom commun (Common Name).
- Les champs suivants sont facultatifs : Adresse électronique, Dir (Répertoire), Challenge password (Mot de passe de vérification) et Company Name (Nom de société).

L'équilibreur de charge Apache crée les fichiers *mypamserver.*csr et *privkey*.pem dans le répertoire actuel.

d. Créez votre clé RSA privée. Pour ce faire, entrez la phrase secrété associée à *privkey*.pem lorsque l'équilibreur de charge vous la demande.

```
openssl rsa -in privkey.pem -out mypamserver.key
```

e. Créez votre certificat.

```
openssl x509 -in mypamserver.csr -out mypamserver.cert -req
-signkey mypamserver.key
```

8. Clôturez l'invite de commande et ouvrez l'explorateur Windows pour copier et supprimer les fichiers générés :

   a. Sélectionnez le dossier *certloc* ou créez un dossier pour y placer le certificat et les fichiers de clé privée.

   b. Ouvrez le dossier *répertoire_installation_apache*\bin, où les fichiers CERT et KEY ont été générés.

   c. Glissez-déposez les fichiers *mypamserver*.cert et *mypamserver*.key dans le dossier *certloc*.

   d. Supprimez les fichiers intermédiaires créés dans le dossier *répertoire_installation_apache/*bin. Il s'agit des fichiers intermédiaires *mypamserver*.CSR, *privkey*.PEM et .RND.

9. Sauvegardez les fichiers que vous avez créés.

10. A l'aide d'un éditeur de texte, modifiez le fichier de texte (*répertoire_installation_apache*\conf\httpd.conf) comme suit :

    a. Supprimer les lignes de commentaire suivantes :

    ```
    Loadmodule rewrite_module modules/mod_rewrite.so

    LoadModule ssl_module modules/mod_ssl.so

    Incluez conf/extra/httpd-ssl.conf
    ```

    b. Ajoutez les lignes suivantes à la fin du fichier httpd.conf. Vous pouvez copier et coller le texte à partir du fichier HTTPD VIRTUALHOST_EXAMPLE que vous avez extrait du dossier compressé SecureDomainConfig_Template.zip.

    ```
    <VirtualHost *:80>
    JkMountFile conf/uriworkermap.properties
    RewriteEngine On
    RewriteCond %{HTTPS} off
    RewriteCond http://%{HTTP_HOST}%{REQUEST_URI}
    !^http://.*c2orepository*|MirroringRequestProcessor*|mirror
    ingrepository*|StartAgent*|genericNoSecurity*|soapAttachmen
    t*
    RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
    </VirtualHost>
    Module d'équilibrage #Load
    Inclure conf/mod-jk.conf
    ```

    c. Enregistrez le fichier httpd.conf modifié et quittez l'éditeur.

11. Sauvegardez les fichiers que vous avez modifiés.

12. A l'aide d'un éditeur de texte, apportez les modifications suivantes au fichier de configuration *répertoire_installation_apache/*conf/extra/httpd-ssl.conf :

    a. Supprimez les marques de commentaire (le cas échéant) dans le texte suivant : Listen 443

    b. Remplacez l'emplacement SSLCertificateFile par .../*certloc/mypamserver.*cert.

    ```
    SSLCertificateFile "/usr/local/certloc/mypamserver.cert"
    ```

    c. Remplacez l'emplacement SSLCertificateKeyFile par .../*certloc/mypamserver.*key.

    ```
    SSLCertificateKeyFile "/usr/local/certloc/mypamserver.key"
    ```

    d. Ajoutez les lignes suivantes à la fin de l'élément <VirtualHost>, avant l'élément </VirtualHost> :

    ```
    SSLOptions +StdEnvVars +ExportCertData
    JkMountFile conf/uriworkermap.properties
    ```

    e. Enregistrez le fichier httpd.conf-ssl modifié et fermez l'éditeur.

13. Redémarrez le service Apache. Pour ce faire, dans le menu Démarrer, cliquez sur Programmes, Apache HTTP Server 2.2, Control Apache Server (Contrôler le serveur Apache), Redémarrer.

    Les modifications sont appliquées.

Annexe F: Exemples de mise à niveau

Ce chapitre traite des sujets suivants :

Exemple : mise à niveau d'un noeud de l'orchestrateur de domaine de la version 3.1 SP01 vers 4.2 sous Windows (page 281)
Exemple : mise à niveau d'un autre noeud de l'orchestrateur de domaine de la version 3.1 SP01 vers 4.2 sous Windows (page 289)
Exemple : mise à niveau d'un orchestrateur non mis en cluster de 4.1 SP01 vers 4.2 sous Windows (page 292)
Mise à niveau d'une version antérieure vers 3.1 SP01 (page 298)

Exemple : mise à niveau d'un noeud de l'orchestrateur de domaine de la version 3.1 SP01 vers 4.2 sous Windows

L'exemple suivant est l'un des deux exemples liés à la mise à niveau d'un orchestrateur de domaine mis en cluster de 3.1 SP01 vers 4.2 sous un système d'exploitation Windows. Les exemples comprennent des captures d'écran sélectionnées et des commentaires pour le scénario suivant :

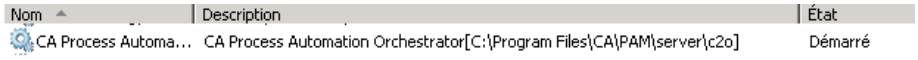
- Noeud d'orchestrateur de domaine 1 - pam-sandbox-n1
- Noeud d'orchestrateur de domaine 2 - pam-sandbox-n2
- Equilibreur de charge de l'orchestrateur de domaine - pam-sandbox-LB

Voici les étapes :

1. Connectez-vous à l'hôte avec le noeud de l'orchestrateur de domaine mis en cluster que vous voulez mettre à niveau.
2. Ouvrez la version de CA Process Automation que vous mettez à niveau. Par exemple, dans le menu Démarrer, sélectionnez Programmes, CA, Domaine CA Process Automation 3.1 SP1, Start CA Process Automation Management Console (Démarrer la console CA Process Automation Management).

   Remarque : Cette méthode simple permet de vérifier que CA EEM est en cours d'exécution et que votre serveur de base de données est actif. Il s'agit d'une condition préalable requise pour la mise à niveau.

3. Cliquez Déconnexion, fermez la console de gestion CA Process Automation et arrêtez le service de l'orchestrateur. Si vous ouvrez Services, vous pouvez vérifier que le statut du service n'est pas défini sur Démarré. Si le statut est défini sur Arrêt en cours, ne poursuivez pas. Actualisez cette vue et patientez jusqu'à ce que le champ Statut soit vide.

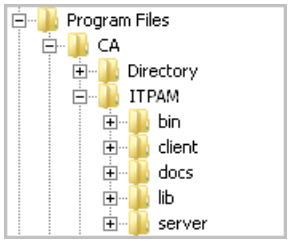


4. Accédez au dossier DVD1 sur le média d'installation et démarrez le fichier Domain_Installer_windows.bat.

5. Pour parcourir les pages initiales de l'assistant de configuration du programme d'installation de composants tiers, cliquez sur Suivant :

   - Bienvenue dans l'assistant de configuration du programme d'installation de composants tiers CA Process Automation
   - Contrat de licence - J'accepte les termes du contrat de licence.

6. Pour l'option Sélectionner le répertoire de destination, accédez au répertoire exact qui contient les fichiers de CA Process Automation 3.1sp01 : bin, client, docs, lib et server. Ce répertoire peut porter le nom par défaut ou un nom fourni préalablement.



Important : Vous devez pointer vers le répertoire correct de sorte que le processus d'installation reconnaisse vos options de configuration précédentes.

7. Dans la fenêtre Conditions préalables à l'installation de CA Process Automation, cliquez sur Suivant pour continuer.

   L'installation des composants tiers commence.

8. Lorsque les fichiers .jar de JDBC pour la page Installation s'affichent, cliquez sur Ajouter des fichiers si vous utilisez un serveur de base de données MySQL ou un SQL Server. Accédez à l'emplacement du fichier .jar approprié.

   Par exemple, le pilote JDBC pour SQL Server a été modifié, accédez à DVD1\drivers\jtds-1.3.jar pour SQL Server.

9. Lorsque la page Fin de l'assistant d'installation de CA Process Automation s'affiche :

   a. modifiez le dernier répertoire du chemin d'accès affiché de DVD1 à DVD2.

CA Process Automation 4.2
Fin de lassistant dinstallation de CA Process Automation
Les éléments requis ont été installés.
Insérez le DVD du programme d'installation de CA Process Automation ou accédez à l'emplacement du contenu du programme d'installation CA Process Automation. Pour lancer l'installation de CA Process Automation, cliquez sur Terminer.
Utiliser un domaine
Répertoire
Administrateur\Desktop\14th november\DVD2\
Parco...
Terminer

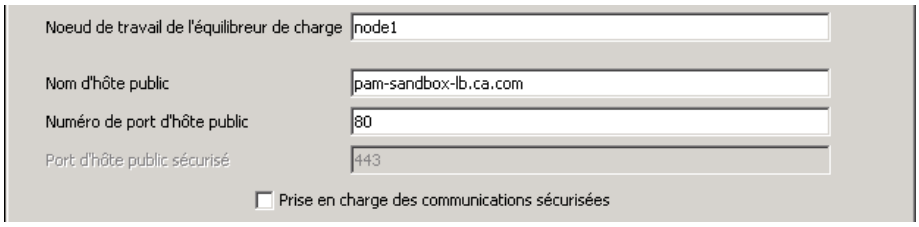
   b. Cliquez sur Terminer.

      Le message Veuillez patienter pendant la copie du programme d'installation de CA Process Automation s'affiche. Cette opération peut prendre quelques minutes.

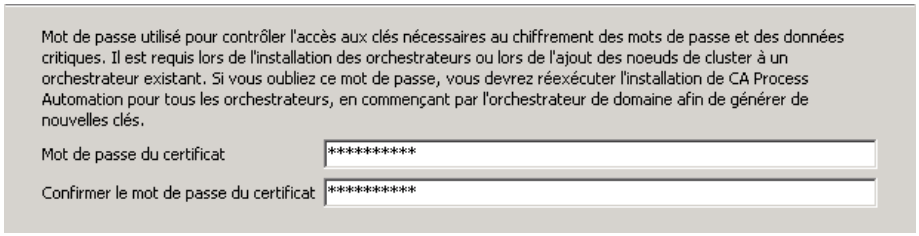
10. Lorsque la fenêtre Bienvenue dans l'assistant d'installation de CA Process Automation s'affiche, cliquez dans les pages initiales de l'assistant :
    - Langue
    - Bienvenue dans l'assistant d'installation de CA Process Automation
    - Contrat de licence - J'accepte les termes du contrat de licence.
    - Répertoire d'accueil Java : il est automatiquement sélectionné, par exemple : C:\Program Files\Java\jdk1.7.0_x.
    - Réinstaller/configurer : l'option Réinstaller signifie **Mettre à niveau**.

      Le message de copie de la configuration s'affiche.
    - Fenêtre Configuration

      L'exemple suivant inclut nos exemples de données :

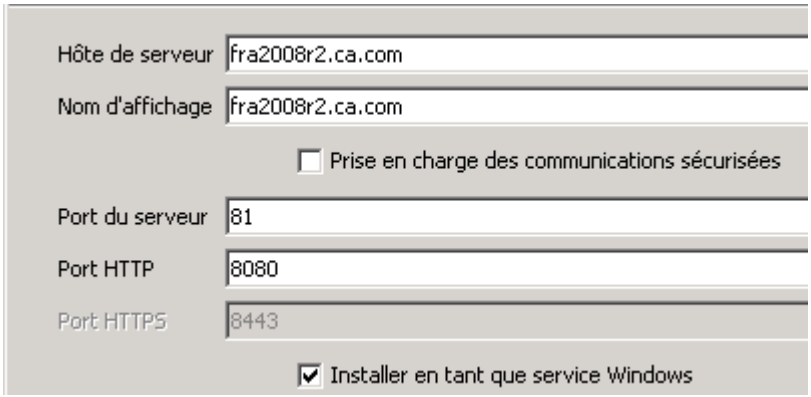


11. Lorsque la fenêtre Définir le mot de passe de certificat s'affiche, saisissez le *même* mot de passe de certificat utilisé dans la version précédente, puis cliquez sur Suivant.

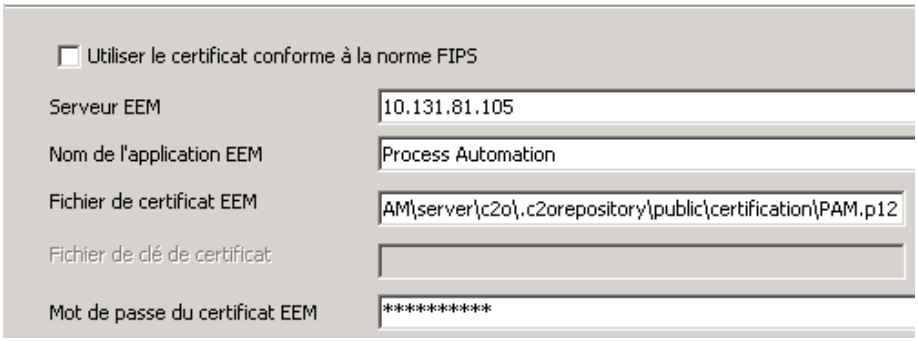

Mot de passe utilisé pour contrôler l'accès aux clés nécessaires au chiffrement des mots de passe et des données critiques. Il est requis lors de l'installation des orchestrateurs ou lors de l'ajout des noeuds de cluster à un orchestrateur existant. Si vous oubliez ce mot de passe, vous devrez réexécuter l'installation de CA Process Automation pour tous les orchestrateurs, en commençant par l'orchestrateur de domaine afin de générer de nouvelles clés.
Mot de passe du certificat
****
Confirmer le mot de passe du certificat
****

12. Cliquez sur Suivant pour sélectionner un dossier du menu Démarrer : la valeur par défaut est CA Process Automation 4.2
13. Pour accéder aux propriétés générales, cliquez sur Suivant. Installer en tant que service Windows est sélectionné par défaut.

    L'exemple suivant inclut nos exemples de données :



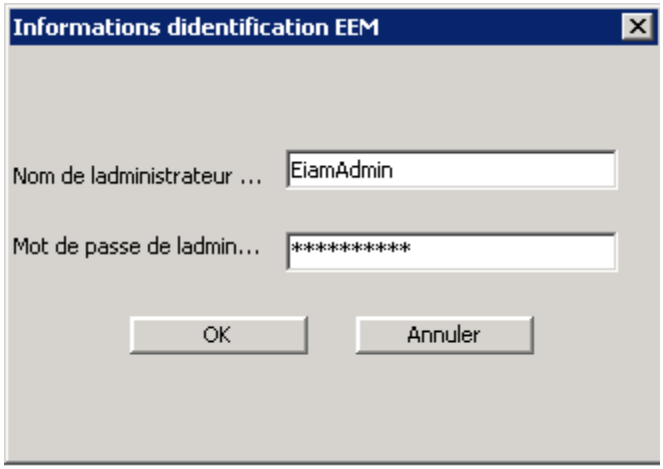
14. Pour accéder aux pages suivantes, cliquez sur Suivant :
    - Répertoire temporaire pour l'exécution des scripts
    - Politique d'exécution PowerShell
15. Lorsque la fenêtre Paramètres de sécurité de CA Embedded Entitlements Manager (CA EEM) s'affiche, les entrées de votre configuration précédente sont remplies par défaut. Exemple :



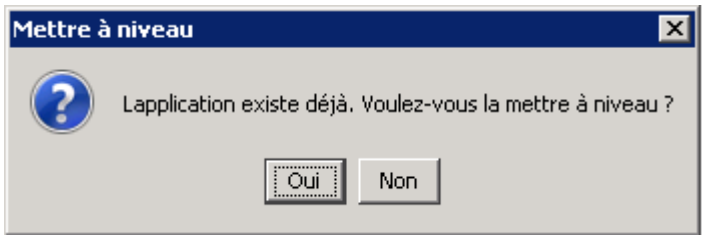
    a. Ignorez le champ Domaine Active Directory par défaut sauf si vous avez configuré CA EEM pour utiliser plusieurs annuaires Microsoft Active Directory. Dans ce cas, saisissez le nom de l'un des annuaires Active Directory que vous avez configurés.

    b. sélectionnez Enregistrer l'application dans CA EEM et cliquez sur Enregistrer.

c. Indiquez les informations d'identification pour vous connecter à CA EEM en tant qu'administrateur EiamAdmin et cliquez sur OK.



d. Cliquez sur Oui pour accepter la mise à niveau.



e. Lorsque le message Application mise à niveau s'affiche, cliquez sur OK.

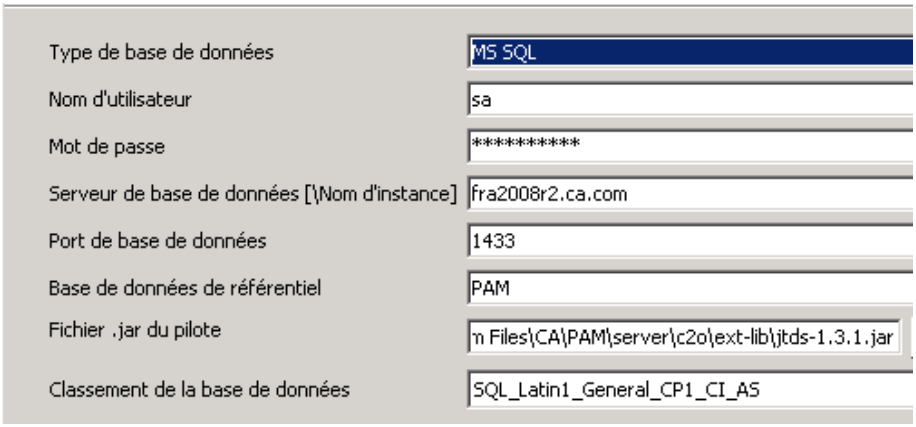
f. (Facultatif) Cliquez sur Tester les paramètres EEM et renseignez Vérifier les paramètres EEM :

- Si vos informations d'identification d'utilisateur sont stockées dans CA EEM, saisissez le nom d'utilisateur et le mot de passe de votre compte d'utilisateur CA Process Automation.
- Si CA EEM utilise Active Directory, entrez vos informations d'identification Active Directory.

Répondez au message de confirmation.

16. Lorsque les paramètres de base de données suivants s'affichent, cliquez sur Tester les paramètres de la base de données pour vérifier que le message Le test a réussi s'affiche. Cliquez sur Suivant.
    - Base de données de référentiel (également appelée base de données de bibliothèque)
    - base de données d'exécution
    - base de données de reporting

    L'exemple suivant inclut nos exemples de données :



17. Pour Fichiers JAR supplémentaires à installer, cliquez sur Suivant ou sélectionnez dans la liste affichée et ajoutez des fichiers supplémentaires si nécessaire.
18. Patientez pendant que le programme d'installation met à niveau (installe) le domaine CA Process Automation.
19. Lorsque la fenêtre Fin de l'assistant d'installation de CA Process Automation s'affiche, cliquez sur Terminer.
20. Connectez-vous au serveur sur lequel node1 de l'orchestrateur de domaine mis en cluster a été mis à niveau.

Remarque : Si vous devez mettre à jour des connecteurs, attendez la fin de cette mise à jour avant de démarrer le service d'orchestrateur.

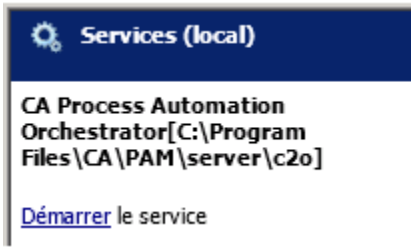
Exemple : mise à niveau d'un autre noeud de l'orchestrateur de domaine de la version 3.1 SP01 vers 4.2 sous Windows

Il s'agit du deuxième exemple lié à la mise à niveau d'un orchestrateur de domaine mis en cluster de 3.1 SP01 vers 4.2 sous un système d'exploitation Windows. Les exemples comprennent des captures d'écran sélectionnées et des commentaires pour le scénario suivant :

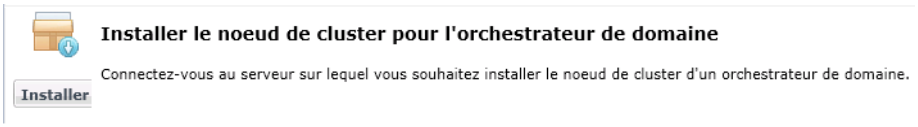
- Noeud d'orchestrateur de domaine 1 - pam-sandbox-n1
- Noeud d'orchestrateur de domaine 2 - pam-sandbox-n2
- Equilibreur de charge de l'orchestrateur de domaine - pam-sandbox-LB

Voici les étapes :

1. Connectez-vous au premier serveur mis à niveau. Démarrez le service d'orchestrateur via Outils d'administration, Services. Notez que le chemin d'accès est identique à l'emplacement dans lequel vous avez initialement installé CA Process Automation.

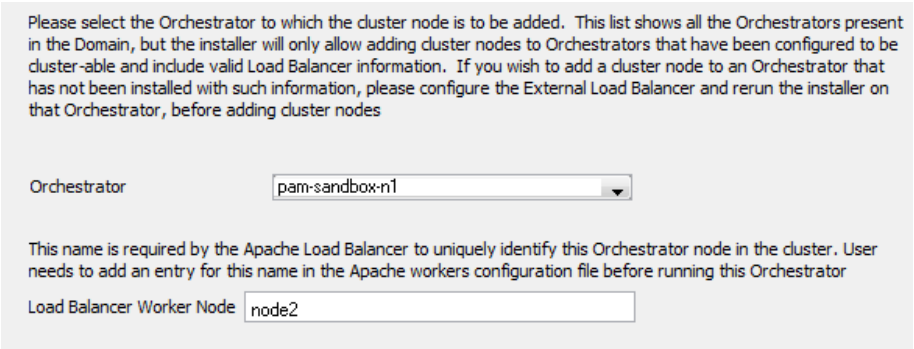


2. Connectez-vous au serveur sur lequel un autre noeud (par exemple, node2) de l'orchestrateur de domaine mis en cluster est installé.
3. Accédez à l'URL du domaine, l'équilibreur de charge de l'orchestrateur de domaine. Dans cet exemple, il s'agit de http://pam-sandbox-lb/itpam.
4. Connectez-vous, cliquez sur l'onglet Configuration, puis sur la palette Installation (en bas à gauche).
5. Sous Installer le noeud de cluster pour l'orchestrateur de domaine, cliquez sur Installation pour lancer la mise à niveau.

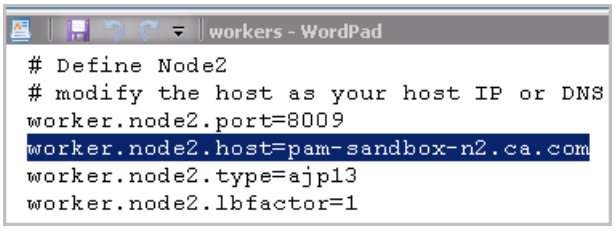

Installer le noeud de cluster pour l'orchestrateur de domaine
Connectez-vous au serveur sur lequel vous souhaitez installer le noeud de cluster d'un orchestrateur de domaine.
Installer

6. La boîte de dialogue Sélection de la langue s'affiche d'abord. Cliquez sur OK.
7. Cliquez dans les pages suivantes de l'assistant :
   - Bienvenue dans l'assistant de configuration du programme d'installation de composants tiers CA Process Automation
   - Contrat de licence : sélectionnez l'option J'accepte les termes du contrat de licence.
   - Sélectionnez Répertoire de destination, par défaut : C:\Program Files\CA\PAM.
   - Conditions préalables à l'installation de CA Process Automation : appelle l'installation.
   - Fin de l'assistant d'installation de CA Process Automation et Utiliser un domaine : cliquez sur Terminer.

     Patientez jusqu'à ce que la page suivante s'affiche. Il n'existe aucun indicateur visuel du traitement précédant l'affichage de la page suivante.
   - Bienvenue dans l'assistant d'installation de CA Process Automation
   - Contrat de licence
8. Si vous avez mis à niveau votre kit de développement Java, accédez au répertoire de base Java, par exemple : C:\Program Files\Java\jdk1.7.0_45.
9. Lorsque la fenêtre Configuration s'affiche,
   a. cliquez sur la liste déroulante Orchestrateur et sélectionnez le premier noeud mis à niveau de l'orchestrateur de domaine.

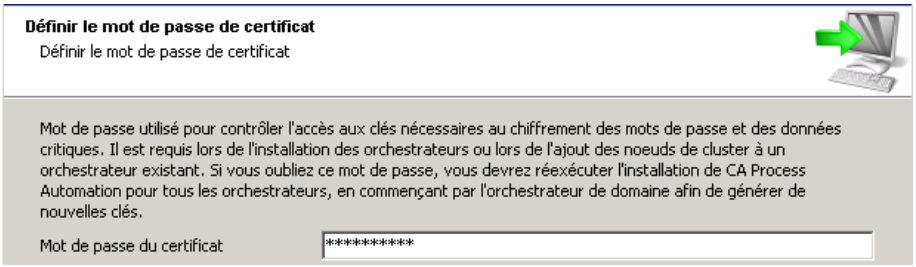

Please select the Orchestrator to which the cluster node is to be added. This list shows all the Orchestrators present in the Domain, but the installer will only allow adding cluster nodes to Orchestrators that have been configured to be cluster-able and include valid Load Balancer information. If you wish to add a cluster node to an Orchestrator that has not been installed with such information, please configure the External Load Balancer and rerun the installer on that Orchestrator, before adding cluster nodes
Orchestrator
pam-sandbox-n1
This name is required by the Apache Load Balancer to uniquely identify this Orchestrator node in the cluster. User needs to add an entry for this name in the Apache workers configuration file before running this Orchestrator
Load Balancer Worker Node
node2

b. Saisissez une valeur dans le champ Noeud de travail de l'équilibreur de charge. Saisissez l'indicateur du noeud (node2, node3, node4) sur lequel vous effectuez la mise à niveau. Tenez compte du format worker.**node2**.host=*hôte actuel,* tel que défini dans le fichier workers.properties du dossier *apache_install_dir/conf*.



Dans cet exemple, le node2 du cluster d'orchestrateur de domaine est défini comme valeur pour worker.**node2**.host=pam-bac dans le fichier sable-n2 en workers.properties. Le nom de domaine complet de l'équilibreur de charge est prérempli dans le champ Nom d'hôte public.

10. Saisissez le nom de votre société.
11. Saisissez le *même* mot de passe de certificat saisi lors de l'installation du noeud précédent de l'orchestrateur de domaine. Il s'agit du *même* mot de passe de certificat utilisé par l'orchestrateur de domaine dans la version antérieure.


Définir le mot de passe de certificat
Définir le mot de passe de certificat
Mot de passe utilisé pour contrôler l'accès aux clés nécessaires au chiffrement des mots de passe et des données critiques. Il est requis lors de l'installation des orchestrateurs ou lors de l'ajout des noeuds de cluster à un orchestrateur existant. Si vous oubliez ce mot de passe, vous devrez réexécuter l'installation de CA Process Automation pour tous les orchestrateurs, en commençant par l'orchestrateur de domaine afin de générer de nouvelles clés.
Mot de passe du certificat
****

12. Cliquez dans les pages suivantes, qui utilisent les paramètres du node1 dans cet exemple.
    - Sélectionnez un dossier du menu Démarrer.
    - Page Propriétés générales (Installer en tant que service Windows ne s'affiche pas, mais elle est prise en compte)
    - Répertoire temporaire pour l'exécution des scripts
    - PowerShell
    - Paramètres de sécurité de CA Embedded Entitlements Manager CA EEM
    - Paramètres de la base de données - Référentiel
    - Paramètres de la base de données - Exécution
    - Paramètres de la base de données - Reporting

    L'installation de la mise à niveau démarre.
13. Lorsque la page Fin de l'assistant d'installation de CA Process Automation s'affiche, cliquez sur Terminer.

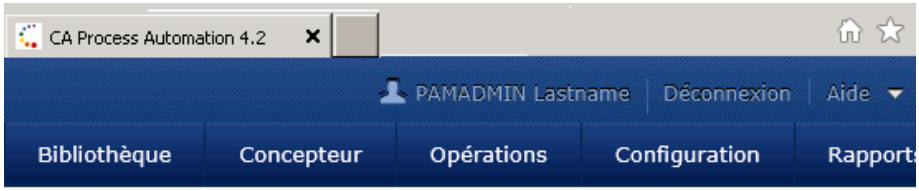
Exemple : mise à niveau d'un orchestrateur non mis en cluster de 4.1 SP01 vers 4.2 sous Windows

L'exemple suivant comprend des captures d'écran sélectionnées semblables à ce qui s'affiche lors de la mise à niveau d'un orchestrateur non mis en cluster de 4.1 SP01 vers 4.2 sous un système d'exploitation Windows. Si vous n'êtes pas familiarisé avec l'assistant d'installation de CA Process Automation, cela peut vous être utile.

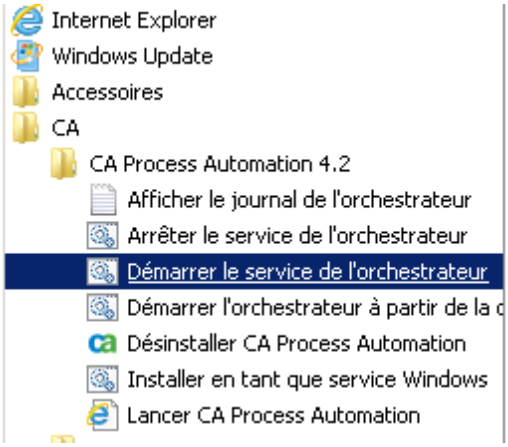
Voici les étapes :

1. Connectez-vous à l'hôte sur lequel l'orchestrateur du domaine est installé.
2. Ouvrez la version de CA Process Automation que vous mettez à niveau. Dans le menu Démarrer, sélectionnez CA, CA Process Automation 4.1 SP01, Démarrer CA Process Automation.

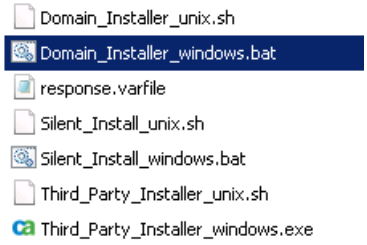
   Remarque : Cette méthode simple permet de vérifier que CA EEM est en cours d'exécution et que votre serveur de base de données est actif. Il s'agit d'une condition préalable requise pour la mise à niveau.



3. Déconnectez-vous de CA Process Automation, fermez le navigateur et arrêtez le service de l'orchestrateur. Par exemple, dans le menu Démarrer, sélectionnez CA, CA Process Automation 4.1 SP01, Arrêter le service de l'orchestrateur. Si vous ouvrez Services, vous pouvez vérifier que le statut du service n'est pas défini sur Démarré.



4. Accédez au dossier DVD1 sur le média d'installation et démarrez le fichier Domain_Installer_windows.bat.



5. Pour parcourir les pages initiales de l'assistant, cliquez sur Suivant :
   - Langue
   - Bienvenue dans l'assistant de configuration du programme d'installation de composants tiers CA Process Automation
   - Contrat de licence - J'accepte les termes du contrat de licence.
   - Sélectionner le répertoire de destination
   - Conditions préalables à l'installation de CA Process Automation

     L'installation commence, y compris celle d'Active MQ et des composants tiers.
   - Installation de fichiers .jar de JDBC. Par défaut, les fichiers .jar de JDBC spécifiés lors de la mise à niveau de l'orchestrateur de domaine sont utilisés.
   - Conditions préalables requises pour l'installation de CA Process Automation

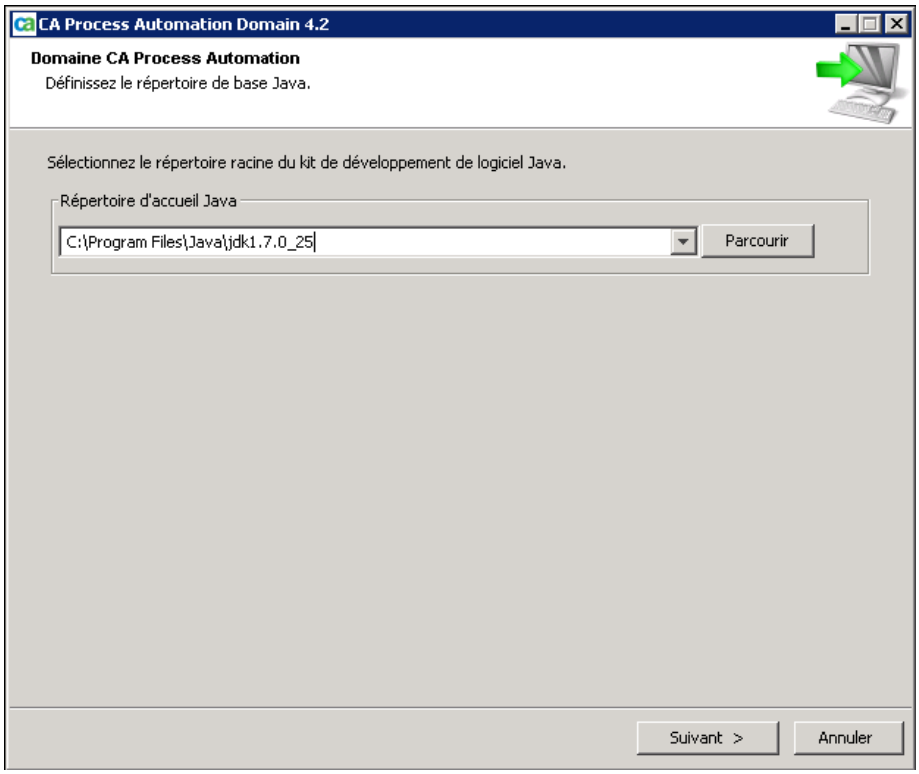
6. Lorsque la fenêtre Fin de l'assistant d'installation de CA Process Automation s'affiche, remplacez DVD1 par DVD2 dans le chemin d'accès au répertoire. Puis, cliquez sur Terminer.

   Le message Veuillez patienter pendant la copie du programme d'installation de CA Process Automation s'affiche. Cette opération peut prendre quelques minutes. Il peut exister un décalage entre la fermeture de cette page et l'ouverture de la page de bienvenue.

7. Lorsque la fenêtre Bienvenue dans l'assistant d'installation de CA Process Automation s'affiche, cliquez dans les pages initiales de l'assistant :

   - Langue
   - Bienvenue dans l'assistant d'installation de CA Process Automation
   - Contrat de licence - J'accepte les termes du contrat de licence.

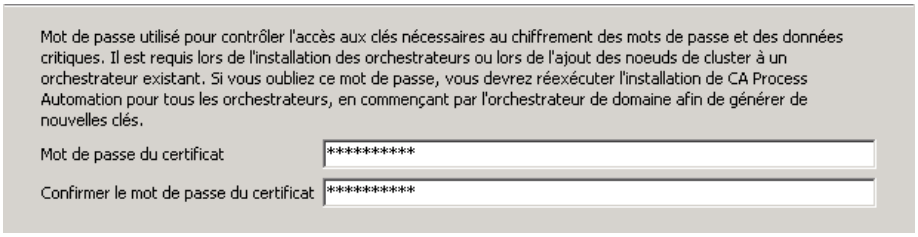
8. Pour le domaine CA Process Automation, définissez le répertoire de base Java, accédez au répertoire correspondant.



9. Pour continuer, cliquez dans les pages :

   - Domaine CA Process Automation, Réinstaller/configurer : la réinstallation est la seule option disponible pour la mise à niveau.
   - Domaine CA Process Automation, fenêtre Configuration

10. Lorsque la page Définir le mot de passe de certificat s'affiche, saisissez le *même* mot de passe de certificat utilisé par l'orchestrateur de domaine. Ce mot de passe de certificat doit correspondre à celui saisi lors de l'installation initiale de cet orchestrateur non mis en cluster. Cliquez sur Suivant


Mot de passe utilisé pour contrôler l'accès aux clés nécessaires au chiffrement des mots de passe et des données critiques. Il est requis lors de l'installation des orchestrateurs ou lors de l'ajout des noeuds de cluster à un orchestrateur existant. Si vous oubliez ce mot de passe, vous devrez réexécuter l'installation de CA Process Automation pour tous les orchestrateurs, en commençant par l'orchestrateur de domaine afin de générer de nouvelles clés.
Mot de passe du certificat
****
Confirmer le mot de passe du certificat
****

11. Cliquez dans Select Start Menu Folder (Sélectionner un dossier du menu Démarrer) pour utiliser votre sélection précédente.
12. Dans la page Propriétés générales, notez les changements suivants dans les valeurs par défaut du port du serveur de l'orchestrateur :

    Port du serveur

    Spécifie le port que l'orchestrateur de domaine utilise pour communiquer avec d'autres orchestrateurs et agents.

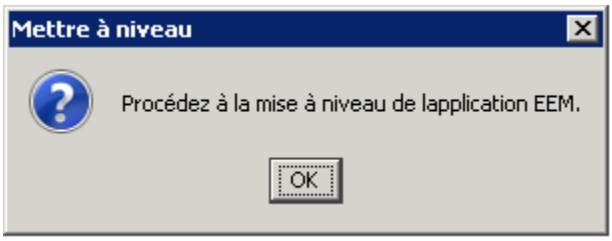
    Valeur par défaut : 80 pour les connexions de base HTTP ou 443 pour les connexions sécurisées HTTPS.

    Port de serveur désapprouvé

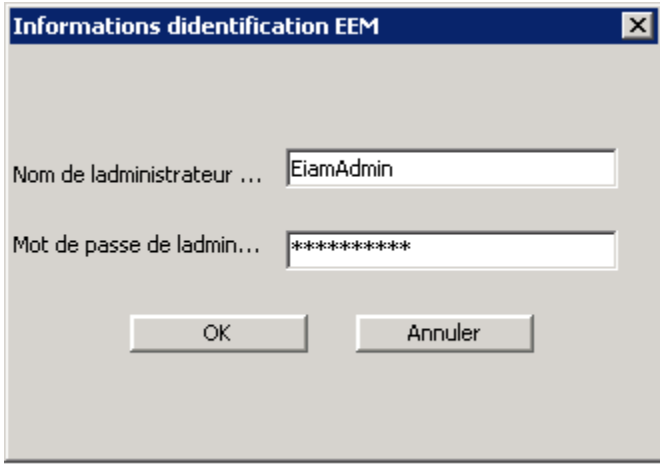
    (Mise à niveau/réinstallation uniquement) Valeur du port de serveur définie pour une version précédente de CA Process Automation.

    Valeur par défaut : 7001
13. Cliquez dans les pages suivantes et apportez les changements comme il vous convient.
    - Répertoire temporaire pour l'exécution des scripts
    - Politique d'exécution PowerShell
14. Lorsque la fenêtre Paramètres de sécurité de CA Embedded Entitlements Manager (EEM) s'affiche,
    a. sélectionnez Enregistrer l'application dans CA EEM et cliquez sur Enregistrer. Il est toujours utile d'effectuer une mise à niveau, car une nouvelle version peut contenir des changements ou des ajouts aux politiques de CA EEM pour CA Process Automation. Lorsqu'aucun changement n'est apporté entre des versions, un message indiquant qu'aucune mise à niveau n'est requise s'affichera.

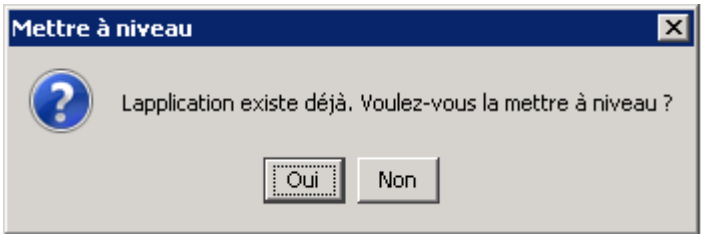
b. Si vous tentez de fermer cette page sans enregistrement et que le processus d'installation détecte une mise à niveau d'une version de CA Process Automation, le processus d'installation vous invitera à sélectionner Enregistrer l'application dans CA EEM et à cliquer sur Enregistrer.



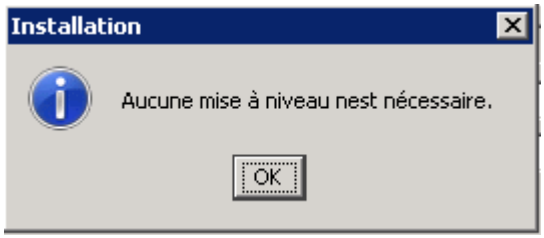
c. Indiquez les informations d'identification pour vous connecter à CA EEM en tant qu'administrateur EiamAdmin.



d. Acceptez la mise à niveau. Le processus d'installation détecte la version du serveur CA EEM et sélectionne le kit de développement logiciel approprié.



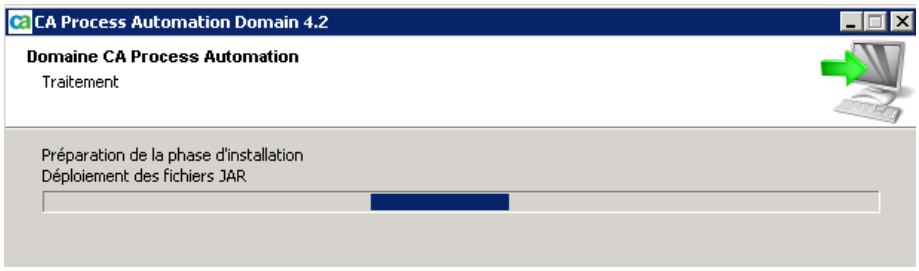
e. Si la mise à niveau n'est pas requise, le message suivant s'affiche :



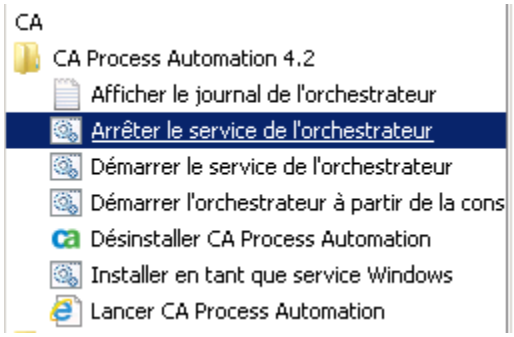
f. Lorsque le message Application enregistrée s'affiche, cliquez sur OK.

15. Cliquez dans Paramètres de la base de données, car ceux-ci ont déjà été définis :
    - Base de données de référentiel
    - base de données d'exécution
    - base de données de reporting
16. Cliquez dans Fichiers JAR supplémentaires à installer si vous n'avez aucun élément à ajouter.

    Le programme d'installation met à niveau (installe) le domaine CA Process Automation.



17. Lorsque la fenêtre Fin de l'assistant d'installation de CA Process Automation s'affiche, cliquez sur Terminer. Consacrez du temps pour l'exécution des mises à jour de schéma avant de démarrer CA Process Automation.
18. Démarrez le service de l'orchestrateur.


CA
CA Process Automation 4.2
Afficher le journal de l'orchestrateur
Arrêter le service de l'orchestrateur
Démarrer le service de l'orchestrateur
Démarrer l'orchestrateur à partir de la cons
Désinstaller CA Process Automation
Installer en tant que service Windows
Lancer CA Process Automation

19. Démarrez CA Process Automation.

CA
CA Process Automation 4.2
Afficher le journal de l'orchestrateur
Arrêter le service de l'orchestrateur
Démarrer le service de l'orchestrateur
Démarrer l'orchestrateur à partir de la
Désinstaller CA Process Automation
Installer en tant que service Windows
Lancer CA Process Automation

Mise à niveau d'une version antérieure vers 3.1 SP01

Vous ne pouvez pas effectuer de mise à niveau directe de CA IT Process Automation Manager (CA IT PAM) 2.x, version de compilation 3.0, or 3.0sp01 vers CA Process Automation 4.2. Vous devez d'abord effectuer une mise à niveau provisoire.

Procédez comme suit :

1. Mise à niveau à partir d'une version antérieure vers CA Process Automation 3.1 SP01
   - CA IT PAM version 2.x
   - CA IT PAM version 3
   - CA IT PAM Service Pack 3.0 SP01

   Remarque : Pour plus d'informations sur la mise à niveau provisoire, téléchargez le Manuel d'installation approprié à partir de l'assistance clientèle.
2. Procédez à la mise à niveau de CA Process Automation Service Pack 3.1 SP01 vers CA Process Automation 4.2 comme indiqué dans la section Procédure de mise à niveau de CA Process Automation (page 142).